HP ProLiant Essentials Vulnerability and Patch Management Pack

User Guide

Part number 367562-004
Fourth edition July 2007

Legal notices

Contents

About this guide

This user guide provides step-by-step instructions for installing and using HP ProLiant Essentials Vulnerability and Patch Management Pack.

Where to go for additional help

In addition to this guide, the following information sources are available.

For additional information about Vulnerability and Patch Management Pack, see:

- http://www.hp.com/go/vpm
- *HP ProLiant Essentials Vulnerability and Patch Management Pack Quick Setup Poster*
- *HP ProLiant Essentials Vulnerability and Patch Management Support Matrix*

For additional information about HP Systems Insight Manager, see:

- http://www.hp.com/go/hpsim
- *HP Systems Insight Manager Installation and User Guide*
- *HP Systems Insight Manager Help Guide*

Website

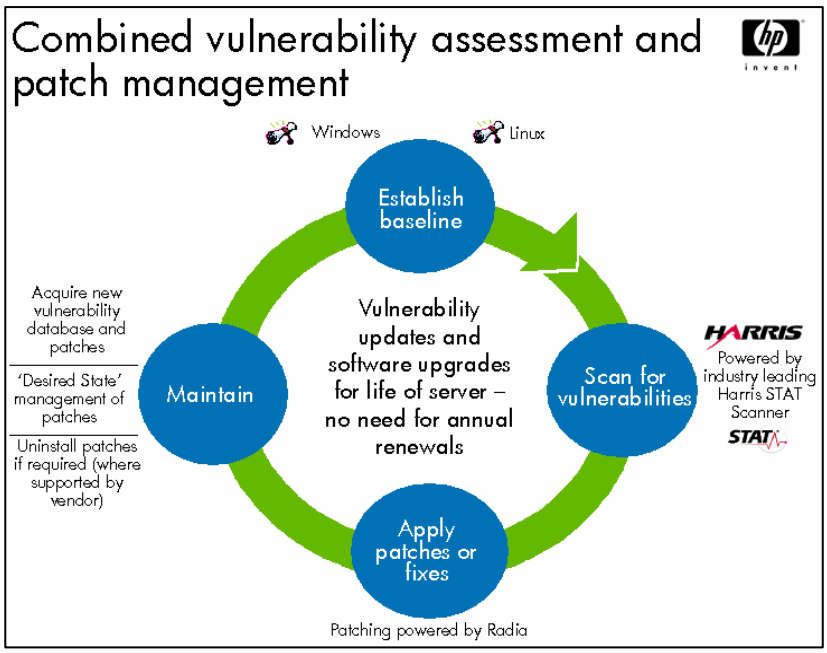
Information about Vulnerability and Patch Management Pack and the latest updates are available at http://www.hp.com/go/vpm.

Introduction

Malicious software security threats are becoming more frequent, more sophisticated, and more costly to businesses, draining billions of dollars in productivity, revenue, and corporate credibility each year. The vast majority of attacks, including automated worms, are performed against known vulnerabilities for which a patch or fix is widely known.

Gain the upper hand in the war against hackers, worms, and trojan software that exploit software security vulnerabilities by using HP ProLiant Essentials Vulnerability and Patch Management Pack—the all-in-one vulnerability assessment and patch management tool. Vulnerability and Patch Management Pack enables you to:

- Enhance system lifecycle management by incorporating vulnerability assessment and patching as an integral part of the system management process
- Accelerate resolution of vulnerabilities by reducing the research time to understand the criticality of the vulnerability and the expected behavior for patches and fixes
- Reduce the risk of security threats by automating the acquisition, scheduling the deployment, and continuously enforcing the persistence (desired state) of patches



Built on industry-leading scanning (PatchLink Security Threat Avoidance Technology) and patch management technology (HP OpenView using Radia), and integrated into the industry-leading HP Systems Insight Manager (HP SIM), Vulnerability and Patch Management Pack delivers a robust set of features.

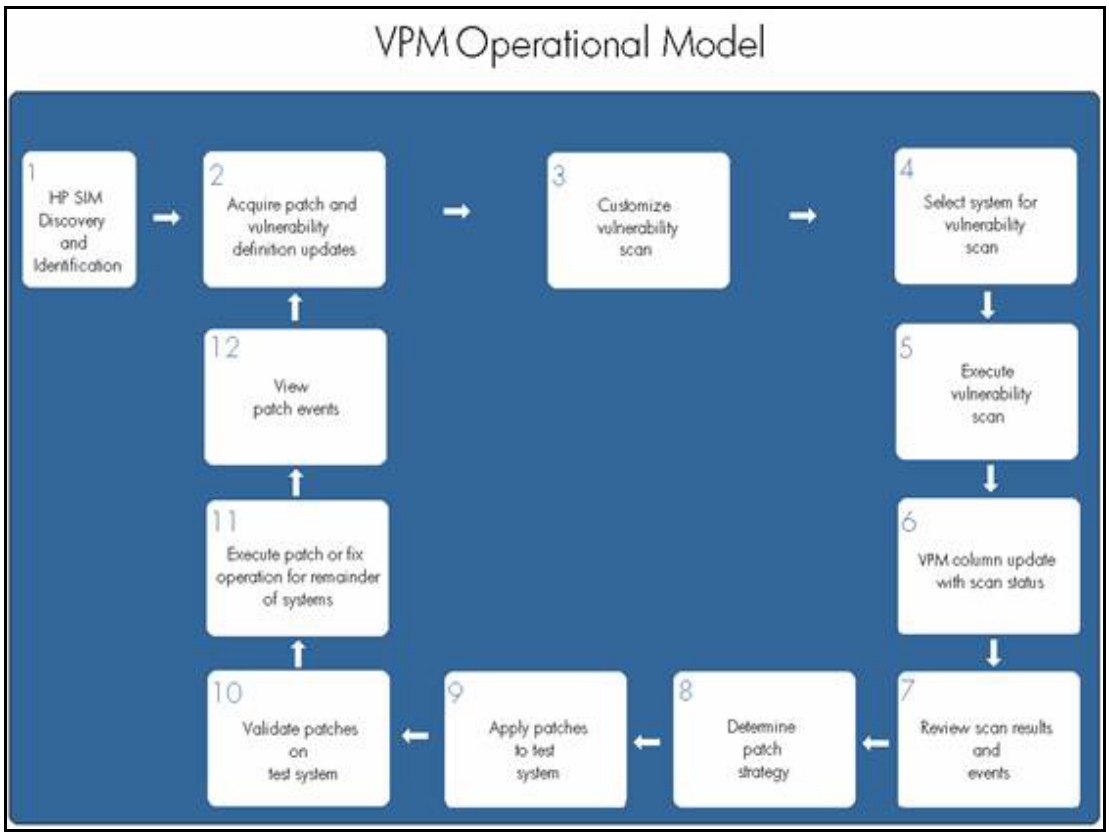
- Combined vulnerability assessment and patch management—A single tool seamlessly combines the assessment and the remediation of vulnerabilities, reducing operational complexity that arises from managing separate tools for vulnerability assessment and patch management.
- Integrated into HP SIM—This enables use of already existing functionality, such as discovery, identification, scheduling, role-based security, notification, and group-based actions, eliminating

the need to recreate these tasks in multiple tools for vulnerability assessment and patch management.

- Comprehensive vulnerability assessment—Coverage of vulnerabilities reported in all leading vulnerability databases ensures comprehensive assessment. Powered by PatchLink Security Threat Avoidance Technology (STAT®) Scanner (the only Common Criteria Certified scanner), the vulnerability assessment identifies vulnerabilities reported in the Common Vulnerabilities and Exposures (CVE) list, the Federal Computer Incident Response Center (FedCIRC) vulnerability catalog, the SANS Top 20 Internet Security Vulnerabilities list, the Computer Emergency Response Team (CERT) advisories list, and the U.S. Department of Energy Computer Incident Advisories Center (CIAC) bulletins.
- Automated acquisition, scheduled deployment, and continous enforcement of patches:
  - Automatically collects new vulnerability updates and patches directly from vendor sources, such as a vendor's Web-based patch repository. Updates can be acquired outside the firewall and imported into the patch repository in infrastructures where firewall policies prevent HTTP and FTP downloads
  - Schedulable deployment, schedulable reboots after deployment, and checkpoint-restarts ensure that patches are deployed with minimal impact on network resources and enable patches to be managed from a central point.
  - Unique desired-state management automatically and continuously ensures that patches remain applied in their proper state. If patches are corrupted in any way, they are automatically reinstalled to bring the system to the desired level of patches.

The Vulnerability and Patch Management Pack process

The following figure details the process for using Vulnerability and Patch Management Pack.



Infrastructure

A server environment using Vulnerability and Patch Management Pack consists of the following components:

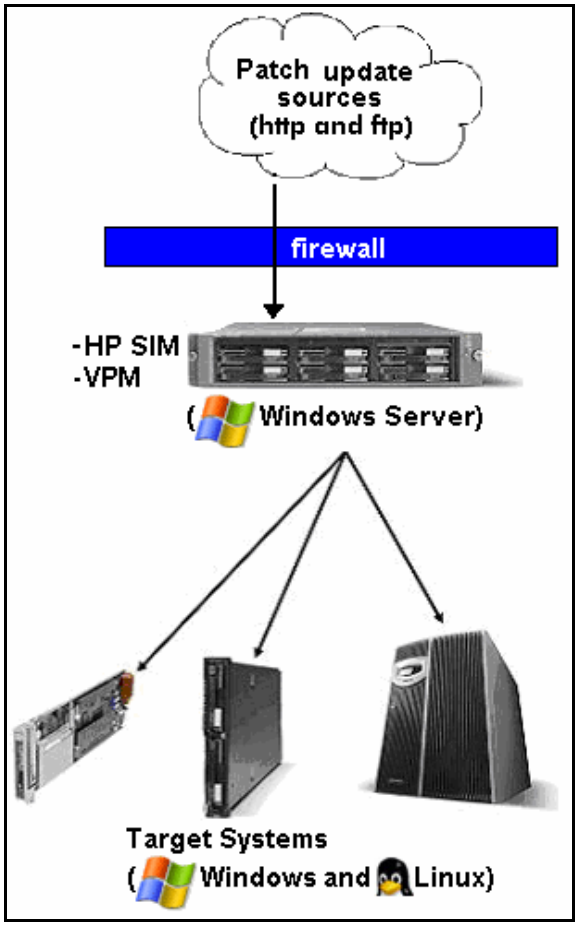
- Vulnerability and Patch Management Pack
- HP SIM
- Target systems
- VPM Acquisition Utility (installed on a separate system, optional)

Vulnerability and Patch Management Pack and HP SIM can be installed together on a single server (referred to as a shared configuration), or each component can be installed on a separate server (referred to as a distributed configuration).

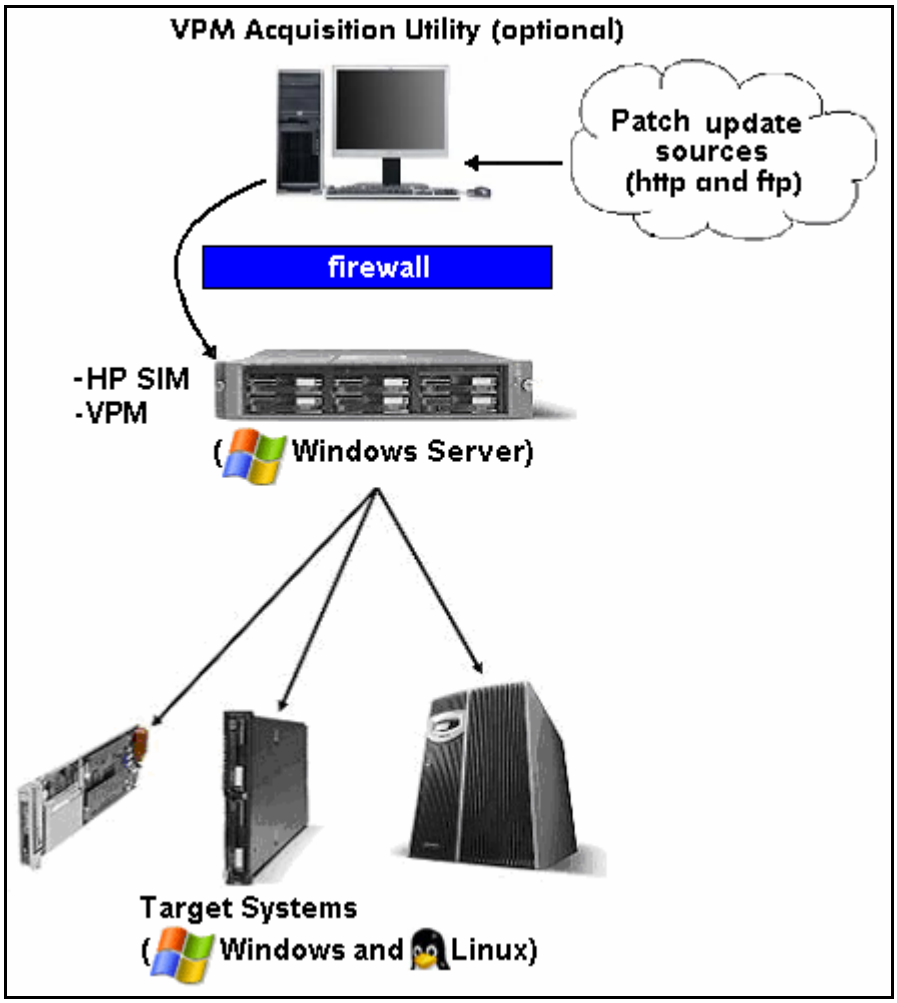
IMPORTANT: For this release, both Vulnerability and Patch Management Pack and HP SIM must be operating on a Microsoft® Windows® server.

Shared server configuration

In a shared server configuration, Vulnerability and Patch Management Pack and HP SIM are installed on the same server. The following figure depicts a shared server configuration, in which the VPM server has Internet access to obtain patch and vulnerability updates.



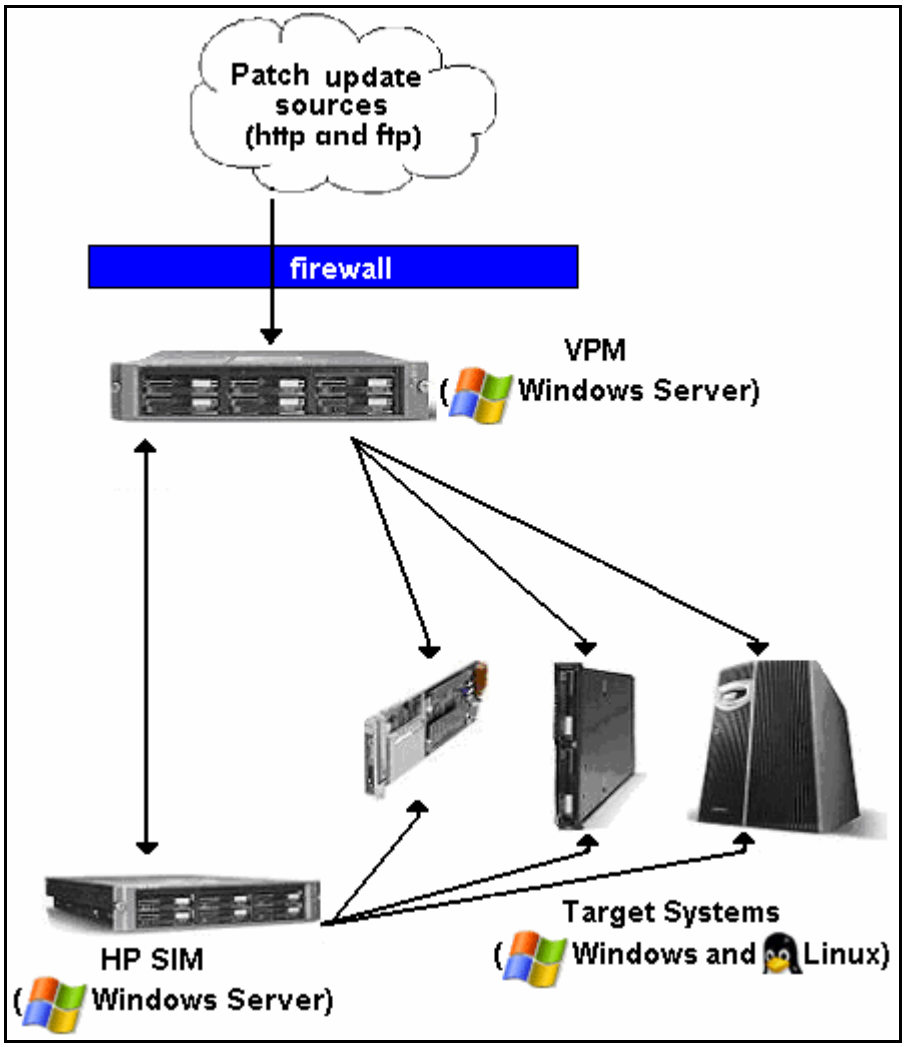
The following figure depicts a shared server configuration, in which the VPM Acquisition Utility is used to obtain patch and vulnerability updates from the patch update sources.



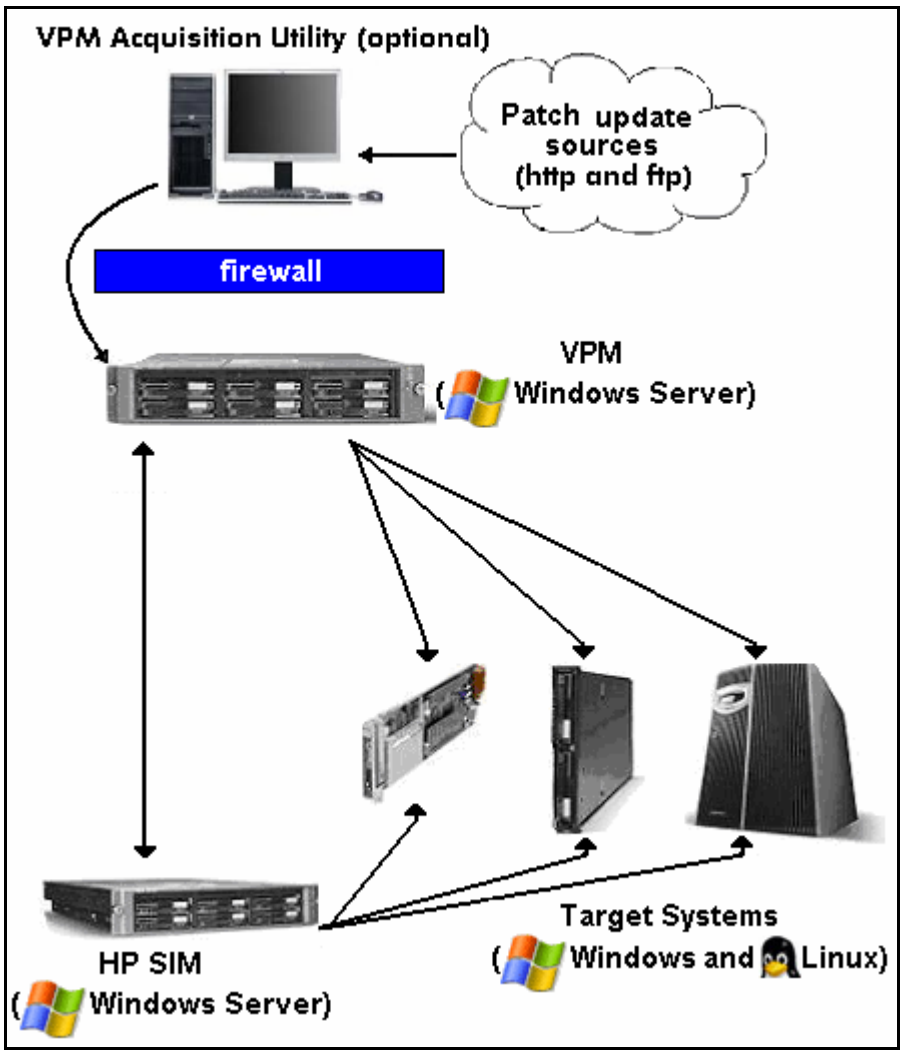
Distributed server configuration

In a distributed server configuration, Vulnerability and Patch Management Pack and HP SIM are each installed on a different server. A distributed server configuration can be beneficial in situations where the hardware limitations of the HP SIM server do not allow Vulnerability and Patch Management Pack to function efficiently on the HP SIM server.

The following figure depicts a distributed server configuration, in which the VPM server has Internet access to obtain patch and vulnerability updates.

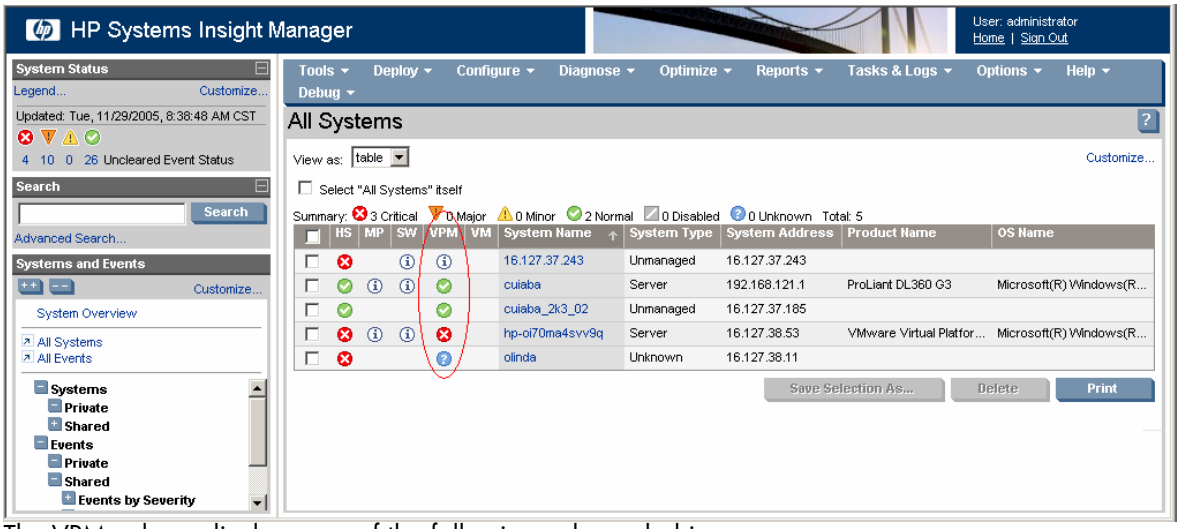


The following figure depicts a distributed server configuration, in which the VPM Acquisition Utility is used to obtain patch and vulnerability updates from patch update sources.



The Vulnerability and Patch Management Pack interface

Vulnerability and Patch Management Pack vulnerability information appears in the VPM column of the HP SIM console, shown circled in the following figure. Initially, the icon depicted in the column displays Vulnerability and Patch Management Pack eligibility information for the target system in the specific row. After target servers are licensed and a vulnerability scan is performed, the column displays the combined status of the last vulnerability scan on the target system (patch status does not appear in the column). Click the icon to display detailed information about the system status with regard to Vulnerability and Patch Management Pack.



The VPM column displays one of the following color-coded icons.

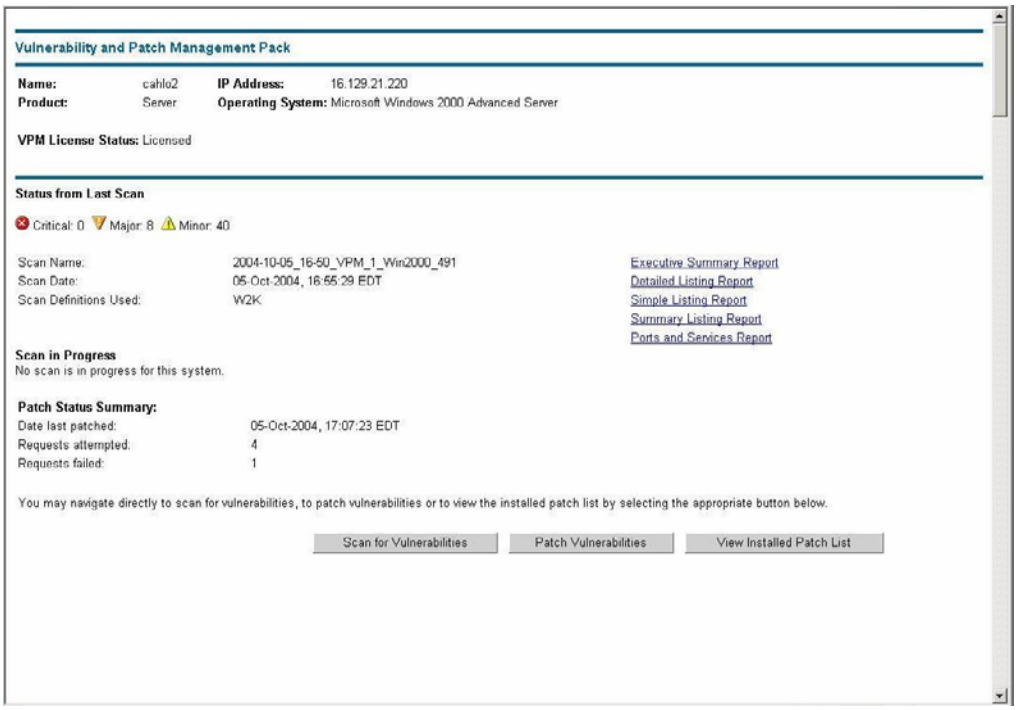
Table 1 Vulnerability and Patch Management Pack icons

Icon	Status	Risk assessment
	Critical vulnerabilities have been detected.	High
	Major vulnerabilities have been detected.	Medium
	Minor vulnerabilities have been detected.	Low and warning
	No vulnerabilities have been detected.	None
	The Unknown icon might appear for the following reasons: • Vulnerability and Patch Management Pack cannot access the system because proper authentication information was not provided. • The system is either not supported or connected. • Vulnerability and Patch Management Pack cannot access the system registry or file system.	Unknown

Table 1 Vulnerability and Patch Management Pack icons

Icon	Status	Risk assessment
	This system is available for licensing, but Vulnerability and Patch Management Pack cannot run for the following reasons: • Vulnerability and Patch Management Pack is not installed. • The system is not licensed. • The system is licensed, but a scan has not yet been performed.	Unknown
No icon	Vulnerability and Patch Management Pack cannot be licensed on this system.	Unknown

Click any status icon to display additional information for the system. Clicking the normal, minor, or major icon opens a new informational page where the last scan results for the system can be accessed. A new scan can also be launched from this page.



Clicking the Unknown icon for a system displays an explanatory page listing possible reasons why status is not available for the system and options to enable Vulnerability and Patch Management Pack.

Requirements

This section lists the hardware and software required for each component in the Vulnerability and Patch Management Pack environment.

A Vulnerability and Patch Management Pack environment consists of the following components:

- Vulnerability and Patch Management Pack
- HP SIM
- VPM Acquisition Utility (optional)
- Target systems

Vulnerability and Patch Management Pack and HP SIM can each be installed on a separate server or together on one server, if the following requirements are met for the server on which each component resides.

Vulnerability and Patch Management Pack

The VPM server, the server on which the Vulnerability and Patch Management Pack software is installed, must meet the following hardware and software requirements. Requirements listed for the VPM server are independent of requirements for HP SIM and any other applications that coexist on the VPM server. For specific hardware and software requirements for the HP SIM server, see the *HP Systems Insight Manager Installation and Configuration Guide*.

Table 2 Hardware requirements

Component	Specification
Any HP x86 server	—
Memory	At least 512 MB RAM
Processor	1.5 GHz or higher
Disk space	1 GB for Vulnerability and Patch Management Pack (150 MB in the TEMP directory for installation)
	Additional space for scan reports and patches
File structure	New Technology File System (NTFS)
DVD-ROM drive	—

Table 3 Software requirements

Component	Specification
Operating system (32-bit versions only)*	Microsoft Windows 2000 Server SP4
	Windows 2000 Advanced Server SP4
	Microsoft Windows Server™ 2003, Standard Edition SP1
	Windows Server 2003, Enterprise Edition SP1
	Windows Server 2003, Web Edition SP1
	Windows® XP Professional SP2
Services	Microsoft Internet Information Services (IIS) 5.0 or later, installed and running**
	TCP/IP, with DNS properly configured so that system names can be resolved to IP addresses
Database	An existing Microsoft SQL Server database can be used, or Microsoft Data Engine (MSDE) will be installed on the VPM server with the Vulnerability and Patch Management Pack installation. When changing databases during an upgrade, patch data from the previous database is not migrated. A full patch acquisition must be performed to repopulate the patch repository.
Applications (must be available on the network)	HP SIM 5.1 or later, installed on a Windows server with Windows Management Interface (WMI) Mapper
	Mozilla Firefox 2.0 or Microsoft Internet Explorer 6.0 or 7.0
	Adobe® Acrobat® Reader 3.*x* or later (to view scan results)

*HP SIM might have additional restrictions for supported service pack levels.

**HP strongly recommends enabling HTTPS if HP SIM and Vulnerability and Patch Management Pack are installed on separate servers. For information about configuring HTTPS service in IIS, see http://support.microsoft.com/?kbid=324069.

HP Systems Insight Manager

HP SIM 5.1 or later must be installed on a Windows server. This release of Vulnerability and Patch Management Pack does not support an HP SIM console operating with a Linux or HP-UX operating system.

VPM Acquisition Utility (optional)

The VPM Acquisition Utility can be installed on a system with Internet access to acquire patch information and patch files from selected vendor websites. This utility allows patch acquisitions and vulnerability updates without requiring the VPM server to be directly connected to the Internet, thereby reducing potential security risks. No other Vulnerability and Patch Management Pack components or database software are required to be installed on the system to download vulnerability and patch updates.

Table 4 lists the minimum requirements for the system on which the VPM Acquisition Utility is installed.

Table 4 VPM Acquisition Utility requirements

Component	Specification
Memory	At least 256 MB RAM
Processor	1.5 GHz or higher
Disk space	12 MB
	Available space for downloading vulnerability patches
Internet access (for downloading vulnerability patches)	
Operating system (32-bit versions only)	Windows 2000 Server SP4
	Windows 2000 Advanced Server SP4
	Windows 2000 Professional
	Windows Server 2003, Standard Edition SP1
	Windows Server 2003, Enterprise Edition SP1
	Windows Server 2003, Web Edition SP1
	Windows XP Professional SP2

Target systems

Target systems are managed by Vulnerability and Patch Management Pack. HP recommends installing HP Management Agents on ProLiant target systems to allow HP SIM to better identify the target systems. Enable WMI or Web-Based Enterprise Management (WBEM) for other target systems. The VPM Patch Agent is automatically deployed when target systems are licensed to allow patches to be applied to the systems.

Secure Shell (SSH) must be installed on Linux target systems.

For a list of supported target systems, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*.

Installation and configuration

This section provides detailed instructions to perform a first-time installation of Vulnerability and Patch Management Pack and the initial configuration steps necessary for use.

Installation location

Vulnerability and Patch Management Pack is installed by default in the C:/Program Files/HP/VPM directory. During the Vulnerability and Patch Management Pack installation, you can either accept this default directory or designate another installation location.

Configuring Microsoft Internet Information Services

Microsoft Internet Information Services (IIS) 5.0 or later must be installed on the intended VPM server to successfully install and use Vulnerability and Patch Management Pack. HP strongly recommends enabling HTTPS if HP SIM and VPM are installed on separate servers.

For information about configuring HTTPS service in IIS, see **http://support.microsoft.com/?kbid=324069**.

Installing Vulnerability and Patch Management Pack

These instructions assume that all hardware and software requirements have been met. Before attempting to install Vulnerability and Patch Management Pack, see the "Requirements" section to verify that all requirements have been met.

HP SIM will be restarted after the Vulnerability and Patch Management Pack installation.

NOTE: This installation might take up to 7 minutes depending on the speed of the server.

Before installing Vulnerability and Patch Management Pack, the following components must be installed, properly configured, and running:

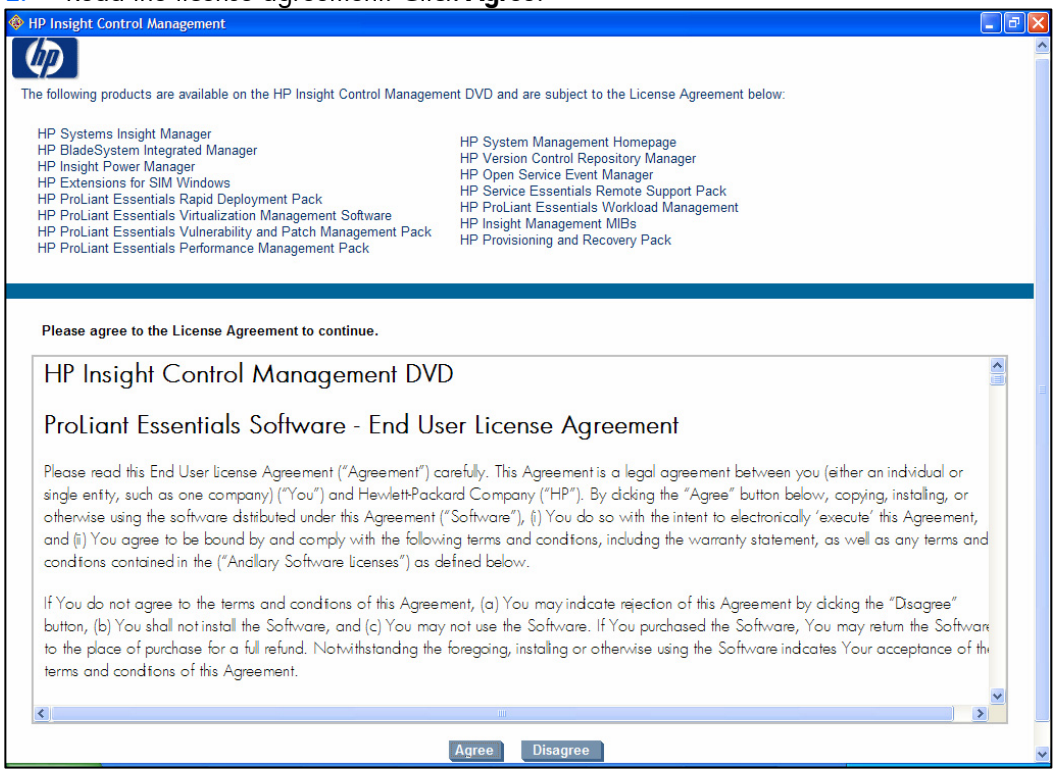
- IIS 5.0 or later
- HP SIM 5.1 or later with WMI Mapper

Be sure to have the following items available before beginning the Vulnerability and Patch Management Pack installation.

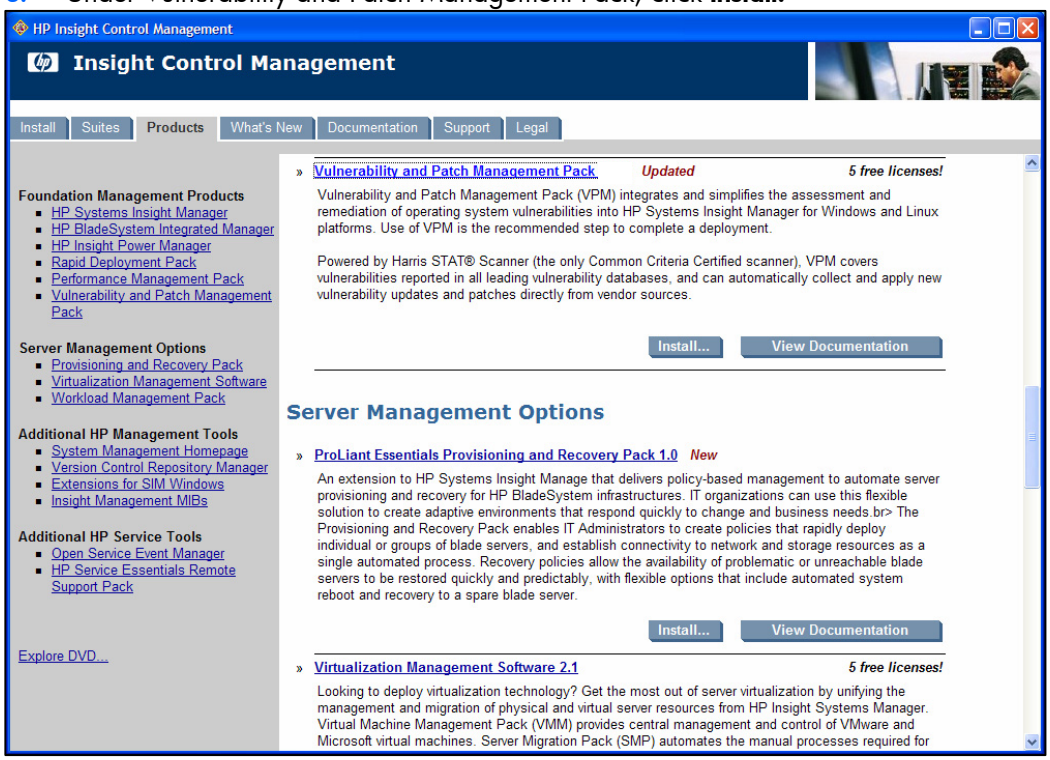
- Location and credentials for HP SIM (user name, password, and domain)
- Credentials for the local server, if installing on other than HP SIM server
- Credentials for the Microsoft SQL Server database, if an existing SQL Server database will be used

Installing from the Insight Control Management DVD

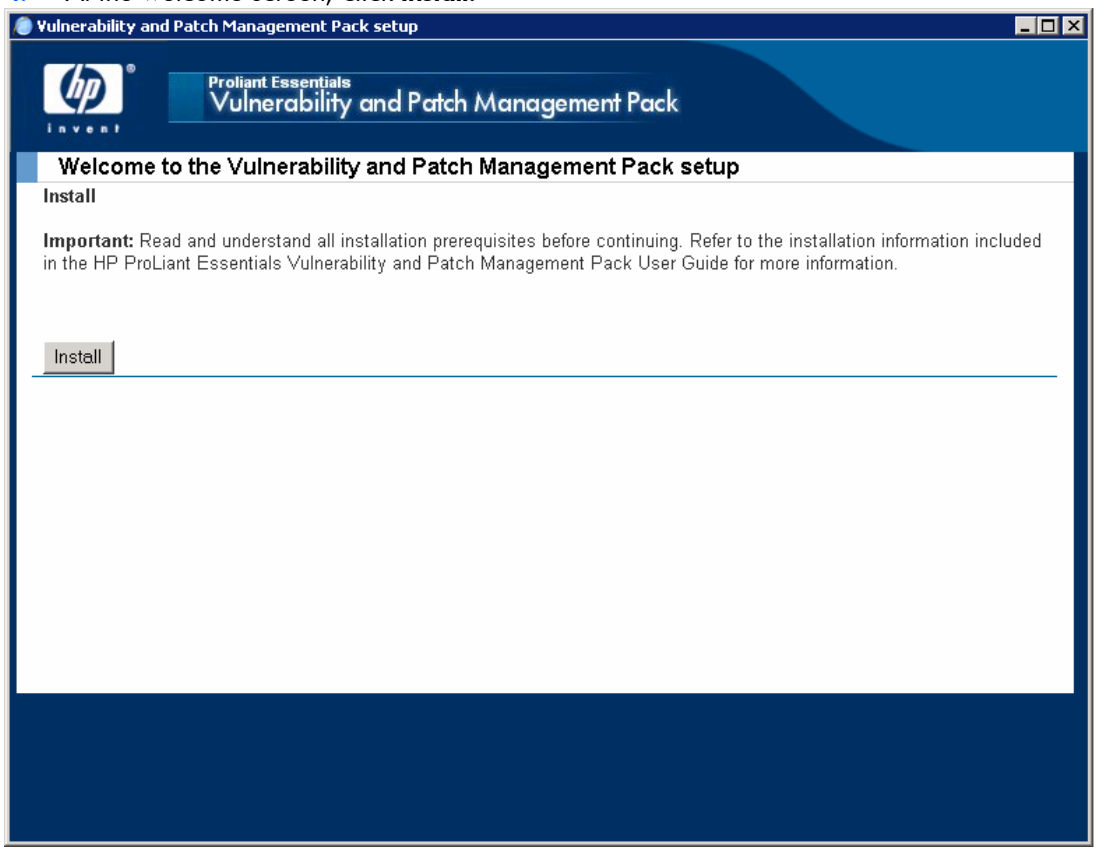
1. Insert the Insight Control Management DVD into the DVD-ROM drive of the intended VPM server. An autorun menu appears.
2. Read the license agreement. Click **Agree**.



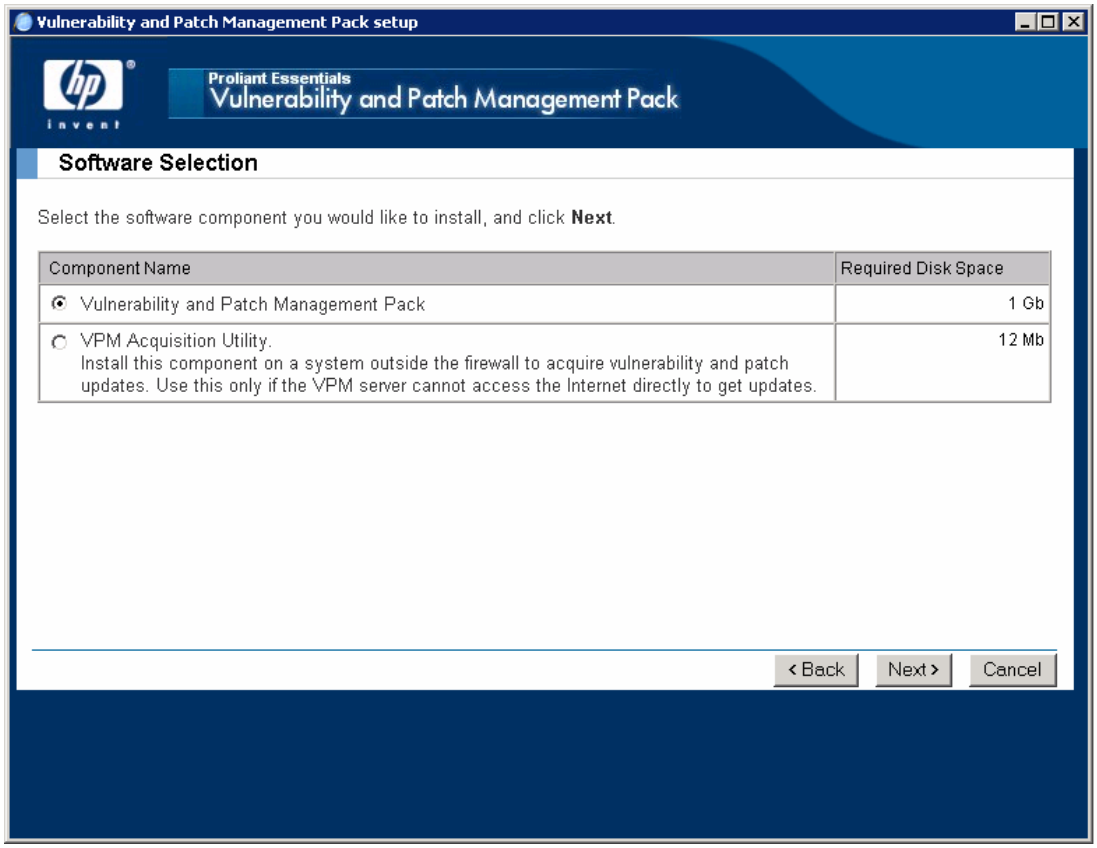
3. Under Vulnerability and Patch Management Pack, click **Install.**



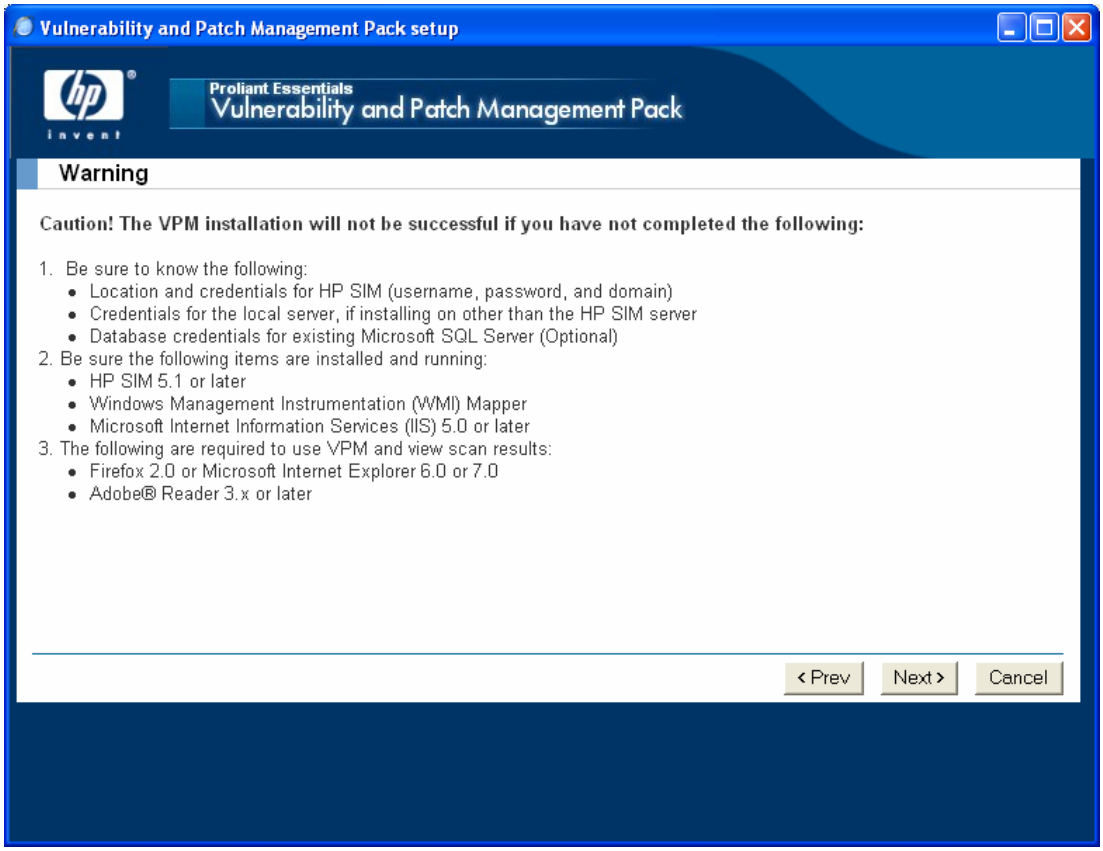
4. At the welcome screen, click **Install.**



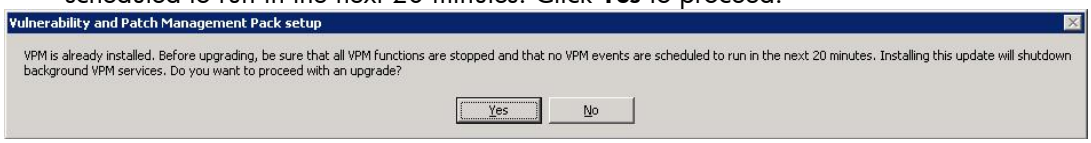
5. At the Software Selection screen, select **Vulnerability and Patch Management Pack,** and click **Next.**



6. Review the requirements, and click **Next**.

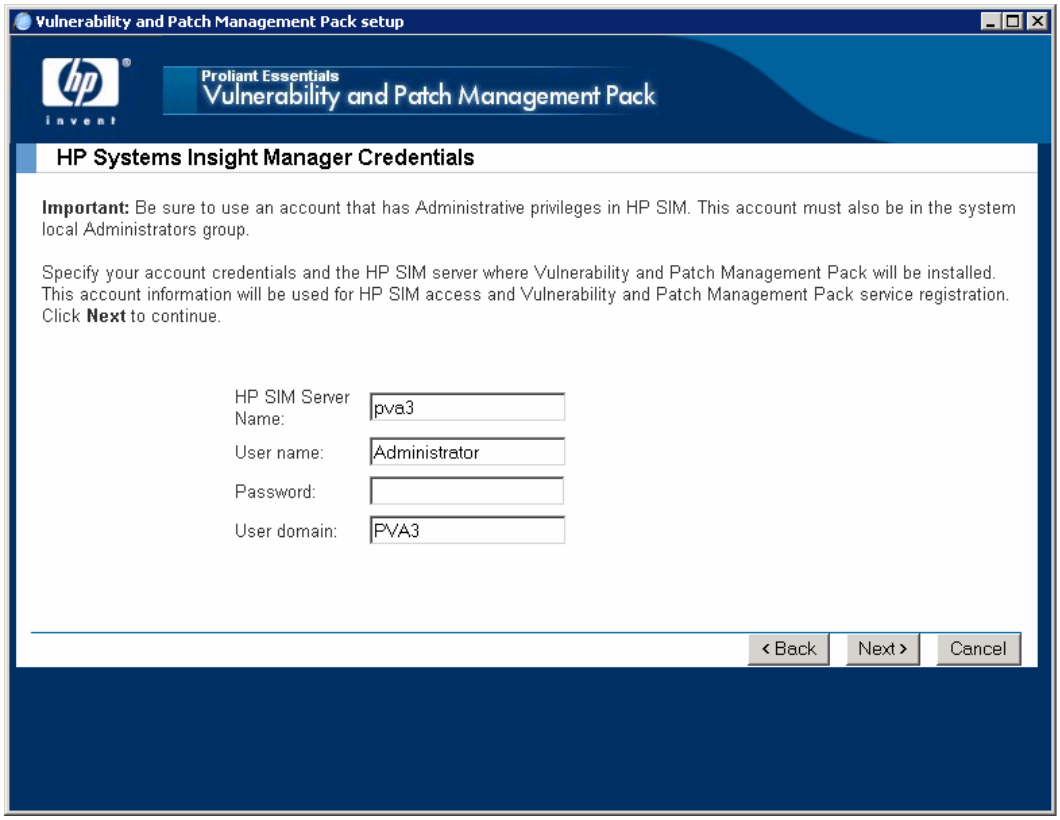


7. If this is an upgrade installation, be sure that all Vulnerability and Patch Management Pack functions are stopped and that no Vulnerability and Patch Management Pack events are scheduled to run in the next 20 minutes. Click **Yes** to proceed.



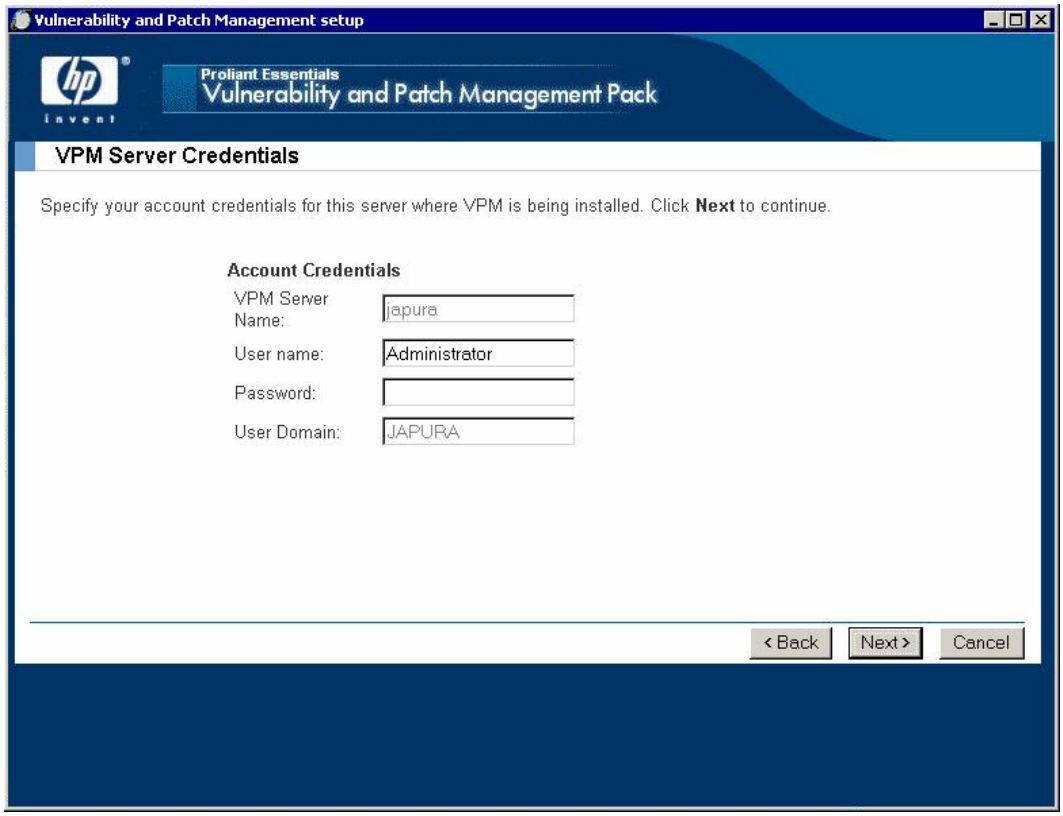
8. Enter the HP SIM account credentials, and click **Next**.

NOTE: This information is entered automatically for an upgrade installation.



9. If Vulnerability and Patch Management Pack is installed on a separate server from HP SIM, enter the user credentials under which Vulnerability and Patch Management Pack will be installed.

NOTE: This information is entered automatically for an upgrade installation. You can only modify the password field.

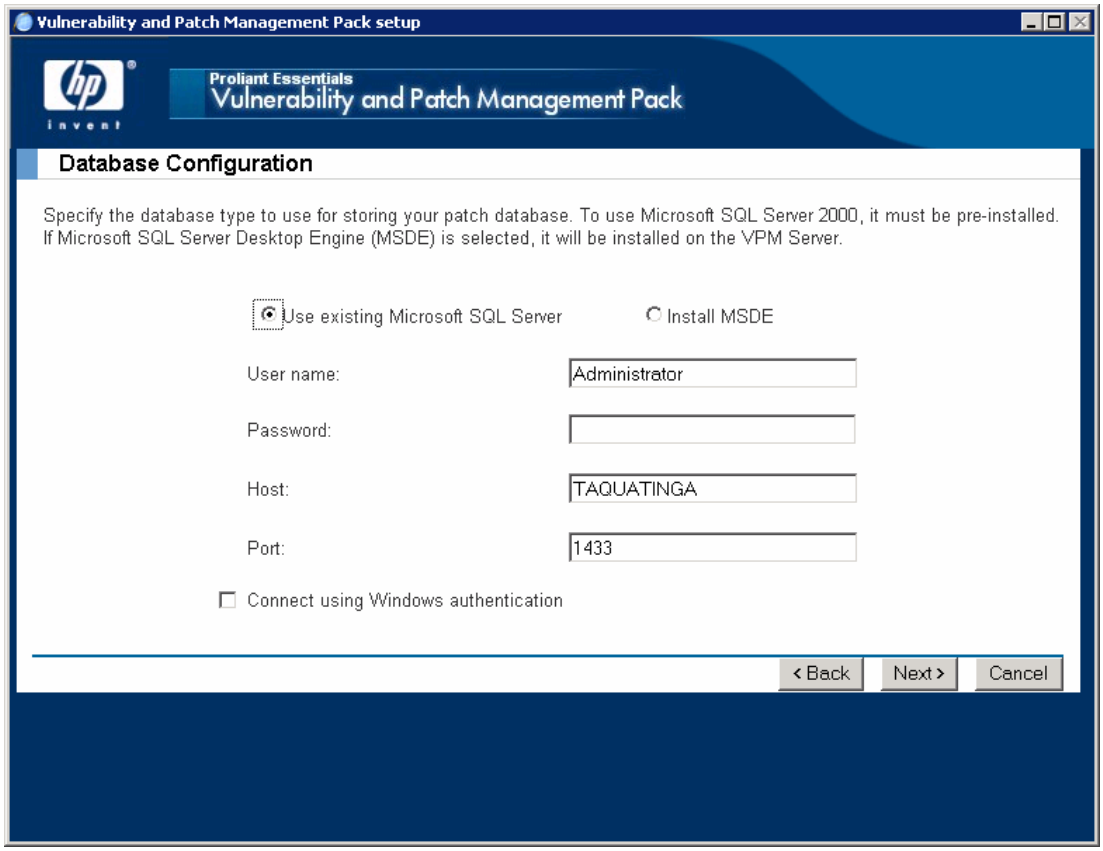


10. Specify the database type to use for storing your patch database, and click **Next.** An existing SQL Server database can be used, or MSDE can be installed on the VPM server.
    - If you select a SQL Server database, enter your database credentials when prompted. The SQL Server database can be accessed using either of the following authentication methods:
      - Windows authentication—The provided credentials must match a Windows account configured with privileges to access the database. The database must be configured to accept Windows authentication.
      - SQL Server authentication—The provided credentials must match a SQL Server account configured with privileges to access the database. The database must be configured to accept SQL Server authentication.

      To use Windows authentication, select the **Connect using Windows authentication** checkbox. Otherwise, SQL Server authentication is used. For information about configuring authentication for your SQL Server database, see the Microsoft SQL Server documentation.

If you select MSDE, and an existing installation of MSDE or files used by MSDE is not current, the server reboots after updated files are installed. Restart the Vulnerability and Patch Management Pack installation from the Insight Control Management DVD.

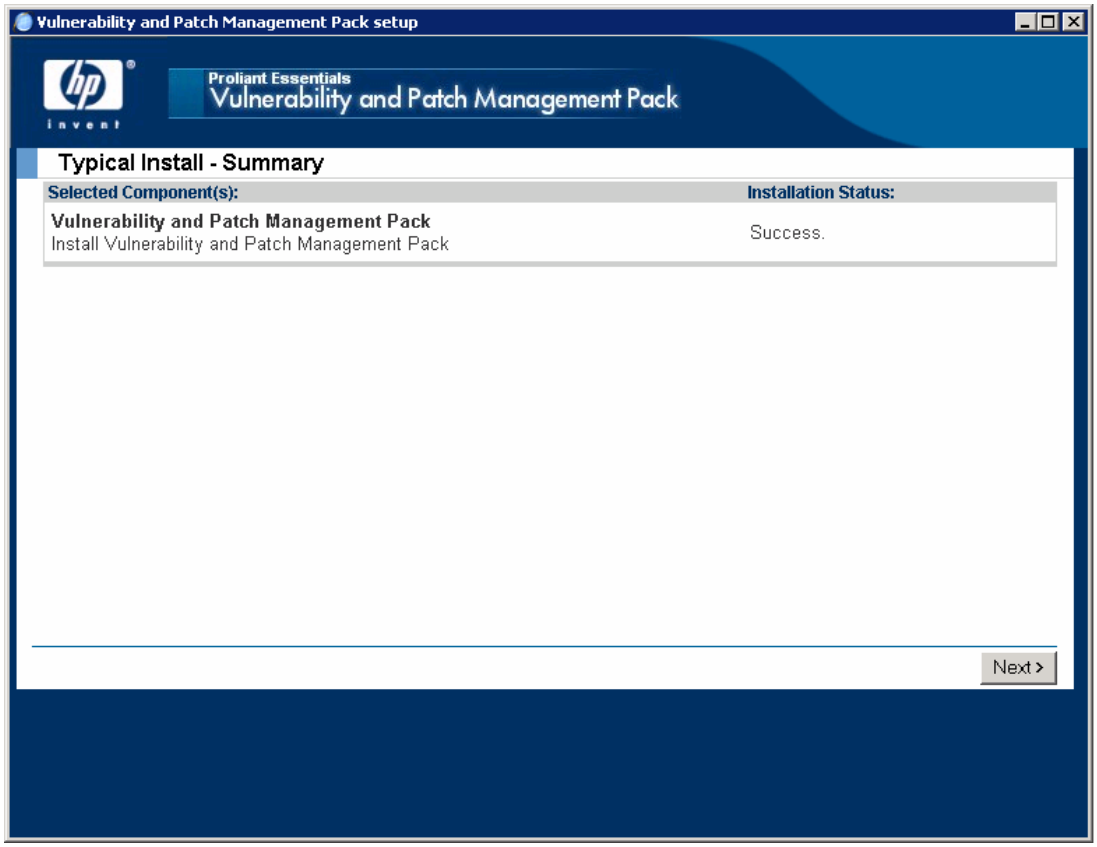
NOTE: The database software is used internally by Vulnerability and Patch Management Pack. No user-accessible data exists in this database.



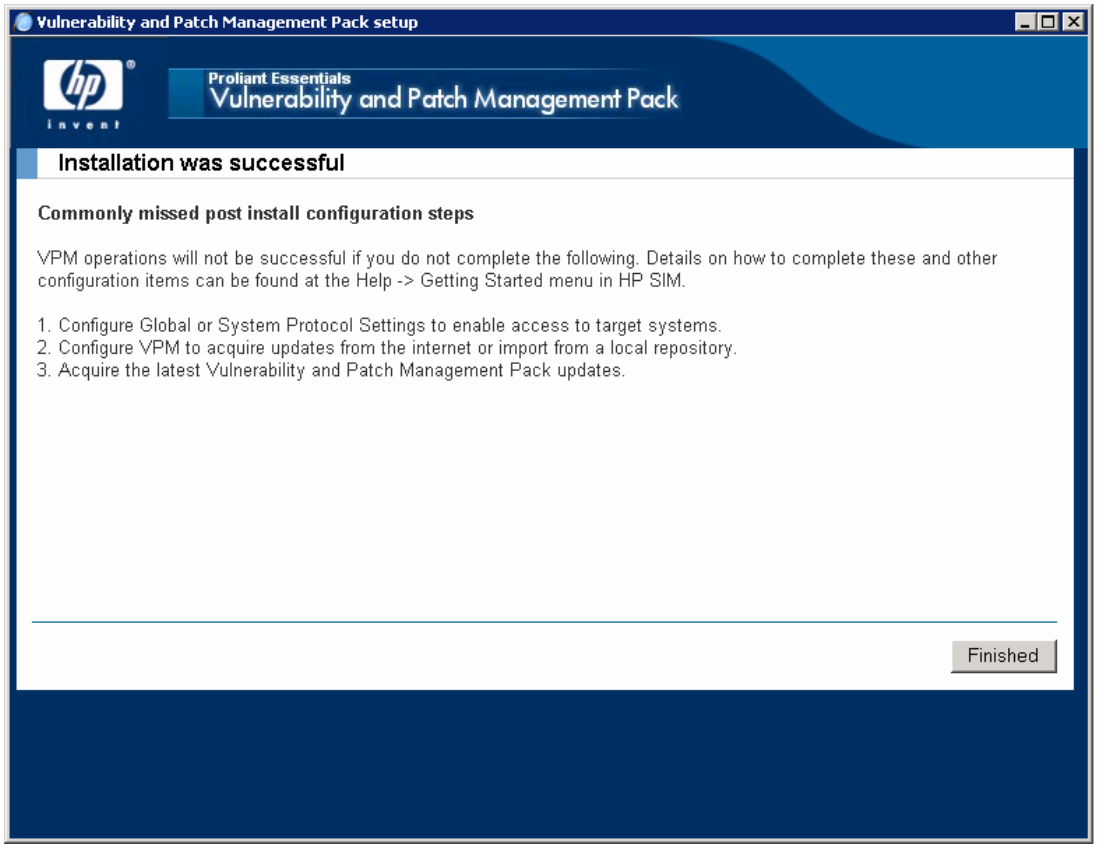
11. Specify the installation directory or accept the default directory.

NOTE: If this is an upgrade installation, the installation directory cannot be changed.

12. Click **Install** at the Typical Install Summary screen to install the Vulnerability and Patch Management Pack software.
13. Click **Next** when the Vulnerability and Patch Management Pack installation completes.



14. Click **Finished.** The HP SIM service is restarted and Vulnerability and Patch Management Pack is available for use.



Installing from the VPM download website

1. After downloading the Vulnerability and Patch Management Pack from the VPM download website, double-click **setup.exe** to start the installation.
2. See steps 4 through 14 in the previous section to complete the installation.

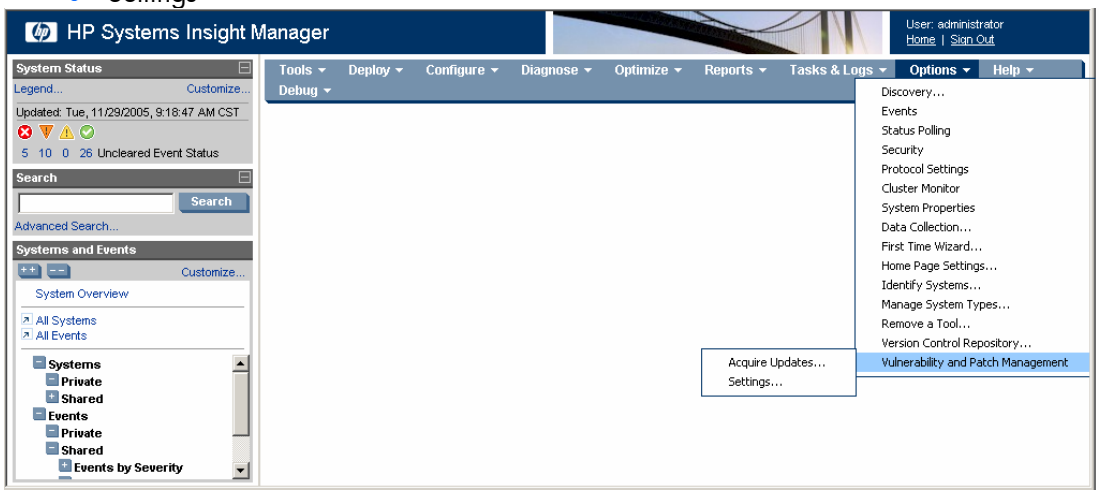
Installed Vulnerability and Patch Management Pack components

Vulnerability and Patch Management Pack installs the following items on the VPM server during installation under Start>Programs>HP Vulnerability and Patch Management Pack:

- Change VPM Credentials
- Uninstall VPM
- VPM Quick Setup Poster
- VPM Release Notes
- VPM Support Matrix
- VPM User Guide

Vulnerability and Patch Management Pack installs the following menu items to the HP SIM toolbar during installation:

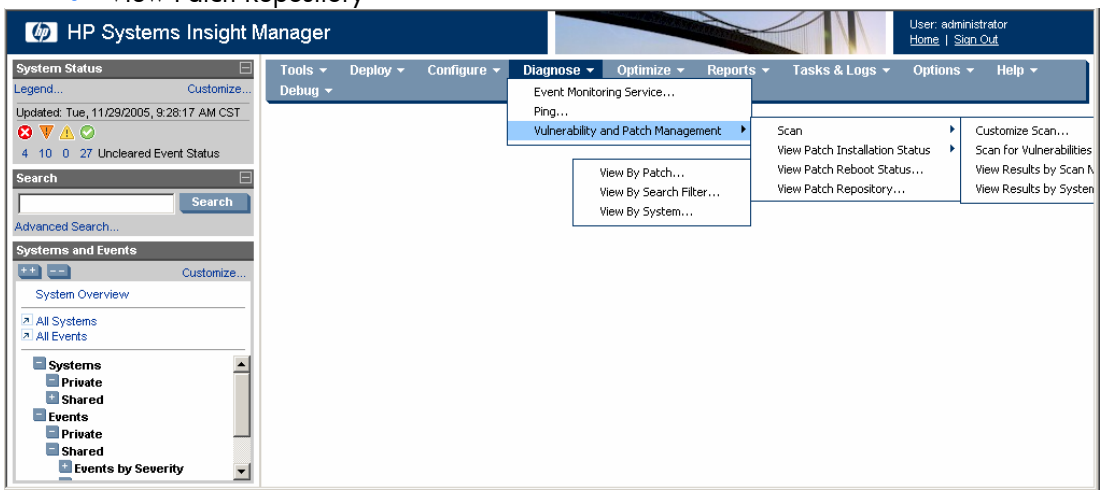
- Options>Vulnerability and Patch Management
  - Acquire Updates
  - Settings



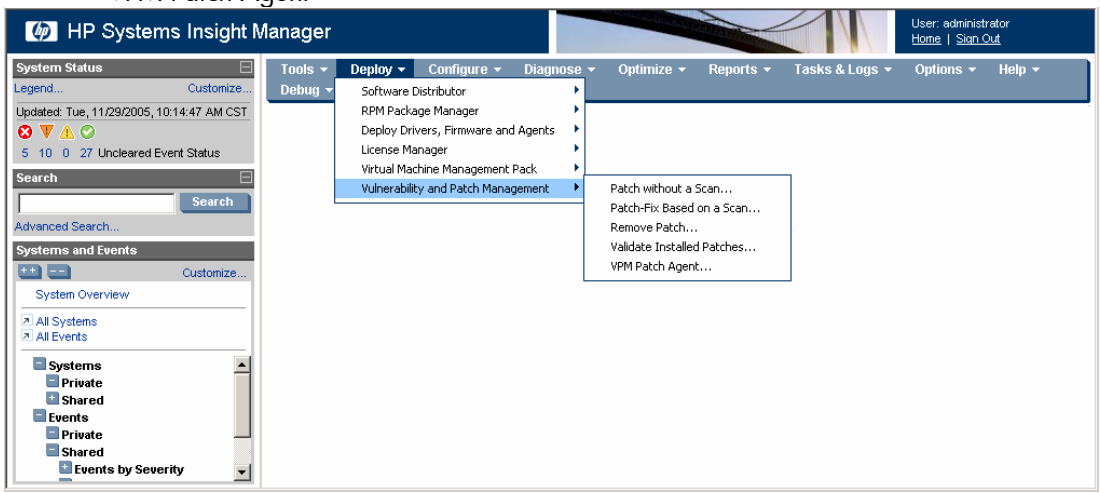
- Diagnose>Vulnerability and Patch Management
  - Scan
    - Customize scan
    - Scan for Vulnerabilities
    - View Results by Scan Name
    - View Results by System
  - View Patch Installation Status
    - View by Patch
    - View by Search Filter

- View by System
- View Patches Installed by VPM

- View Patch Reboot Status
- View Patch Repository



- Deploy>Vulnerability and Patch Management
  - Patch without a Scan
  - Patch-Fix Based on a Scan
  - Remove Patch
  - Validate Installed Patches
  - VPM Patch Agent



Vulnerability and Patch Management Pack upgrades

New versions of Vulnerability and Patch Management Pack are automatically installed over a previous version. Any scheduled tasks, scan reports, and patch updates are retained. Vulnerability and Patch Management Pack supports installation with an existing SQL Server database. However, patch data from a previous database is not migrated. A full patch acquisition must be performed to repopulate the patch repository.

For detailed information about a particular version, see the release notes.

For more information, critical updates, and the latest version of the software, click **Download** at http://www.hp.com/go/vpm.

Vulnerability scan definitions are updated frequently as new information about security issues is made available. Sign up for e-mail notifications of vulnerability definition updates or Vulnerability and Patch Management Pack updates at http://www.hp.com/go/swupdate.

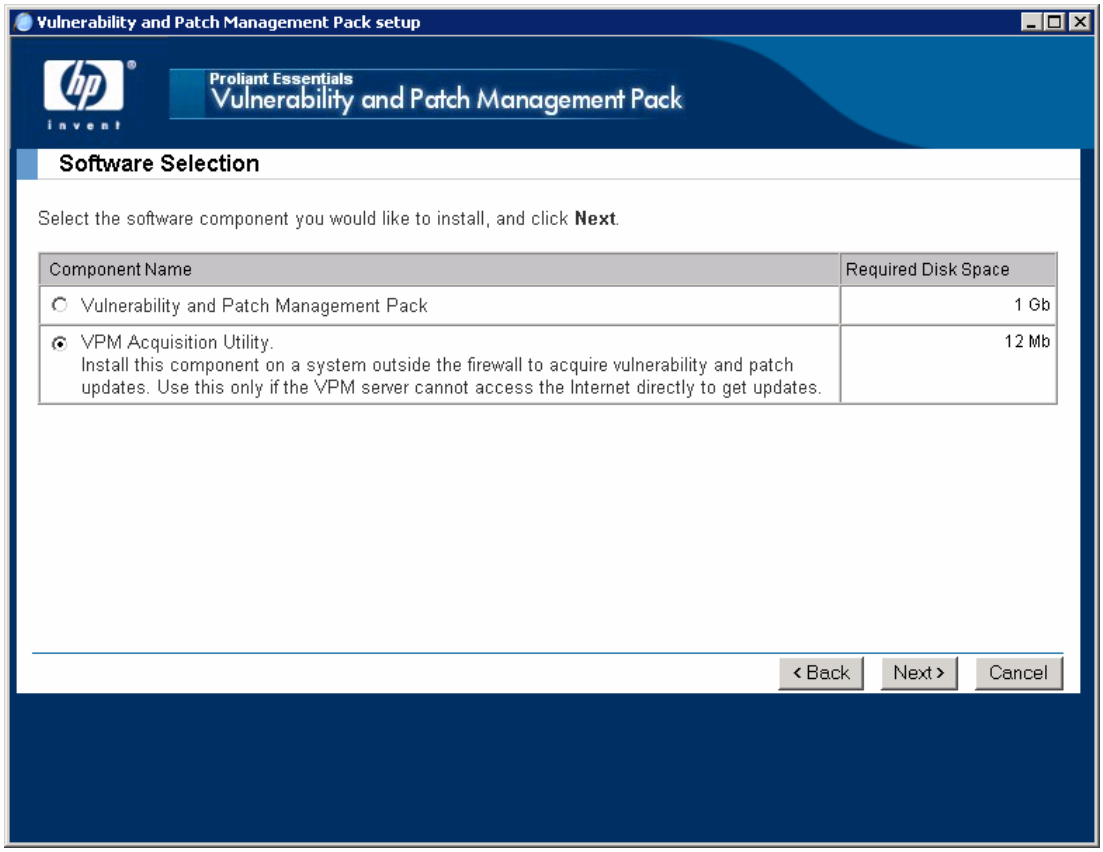
Installing the VPM Acquisition Utility (optional)

If your VPM server is not directly connected to the Internet, the VPM Acquisition Utility can be installed on any system with Internet access to acquire vulnerability and patch updates.

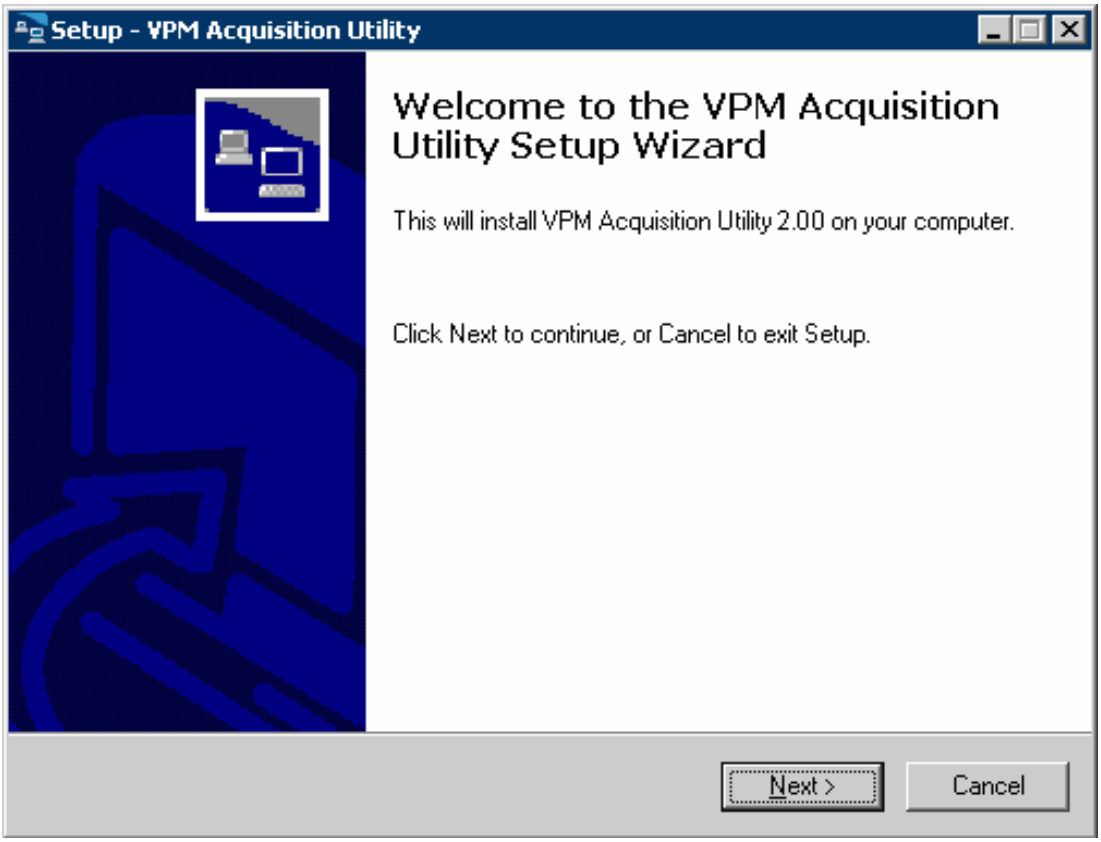
IMPORTANT: In both a distributed and shared configuration, the VPM Acquisition Utility cannot be installed on the VPM server or the HP SIM Central Management System (CMS).

To install the VPM Acquisition Utility:

1. Insert the Insight Control Management DVD into the DVD-ROM drive of the system where patch and vulnerability updates will be obtained. An autorun menu appears.
2. Read the license agreement. Click **Agree**.
3. Under HP ProLiant Essentials Vulnerability and Patch Management Pack, click **Install.**
4. At the welcome screen, click **Install.**
5. At the Software Selection screen, select **VPM Acquisition Utility,** and click **Next.**

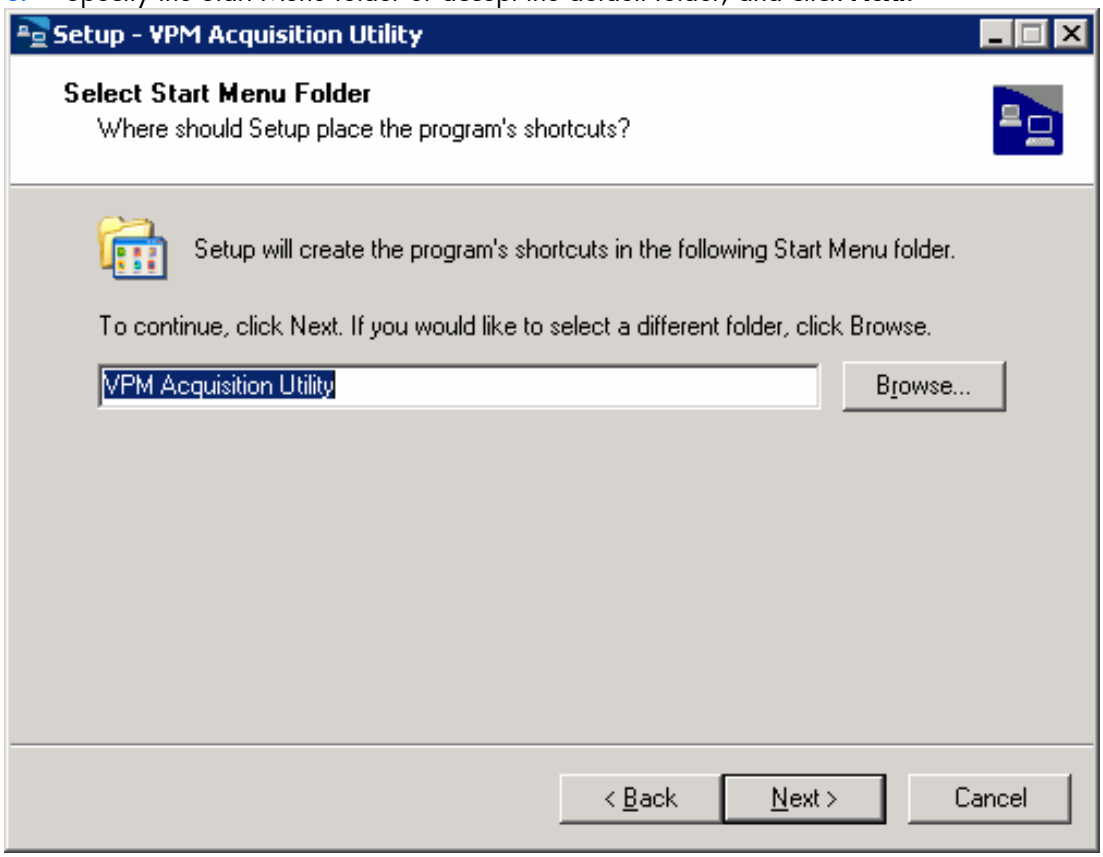


6. Click **Next**.

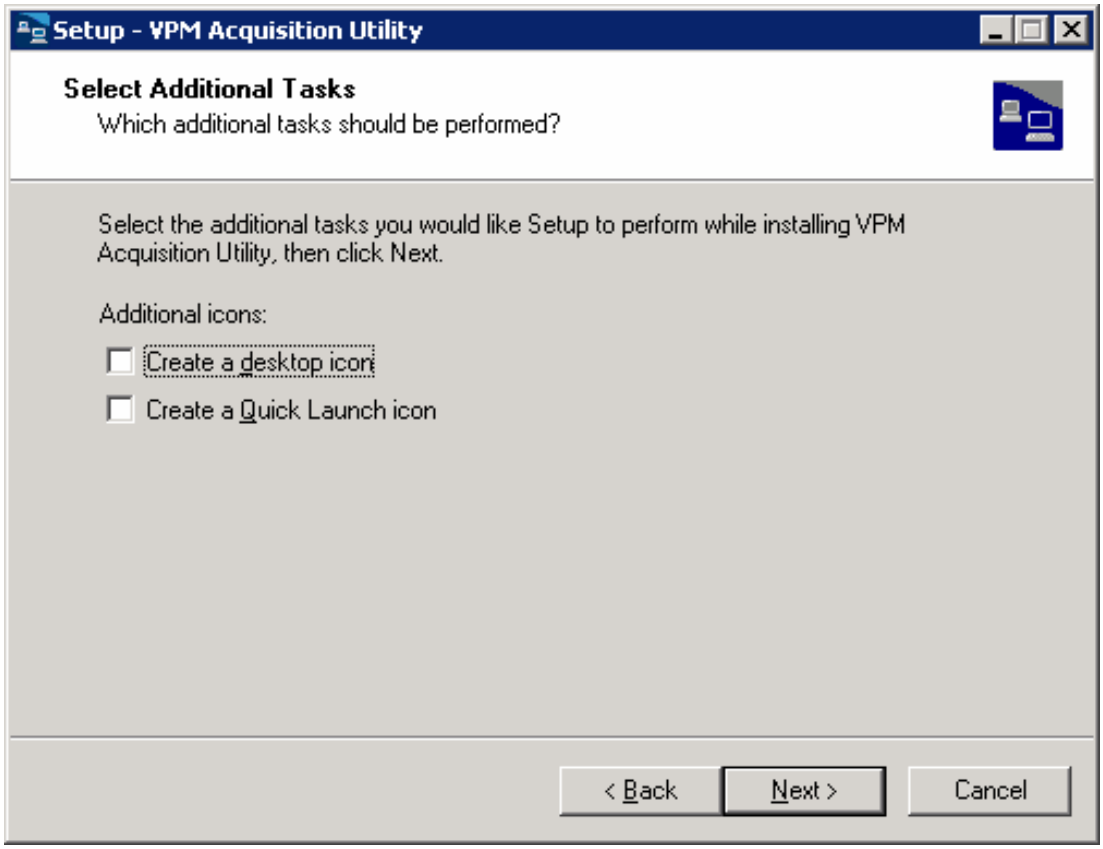


7. Specify the installation directory or accept the default directory, and click **Next.**

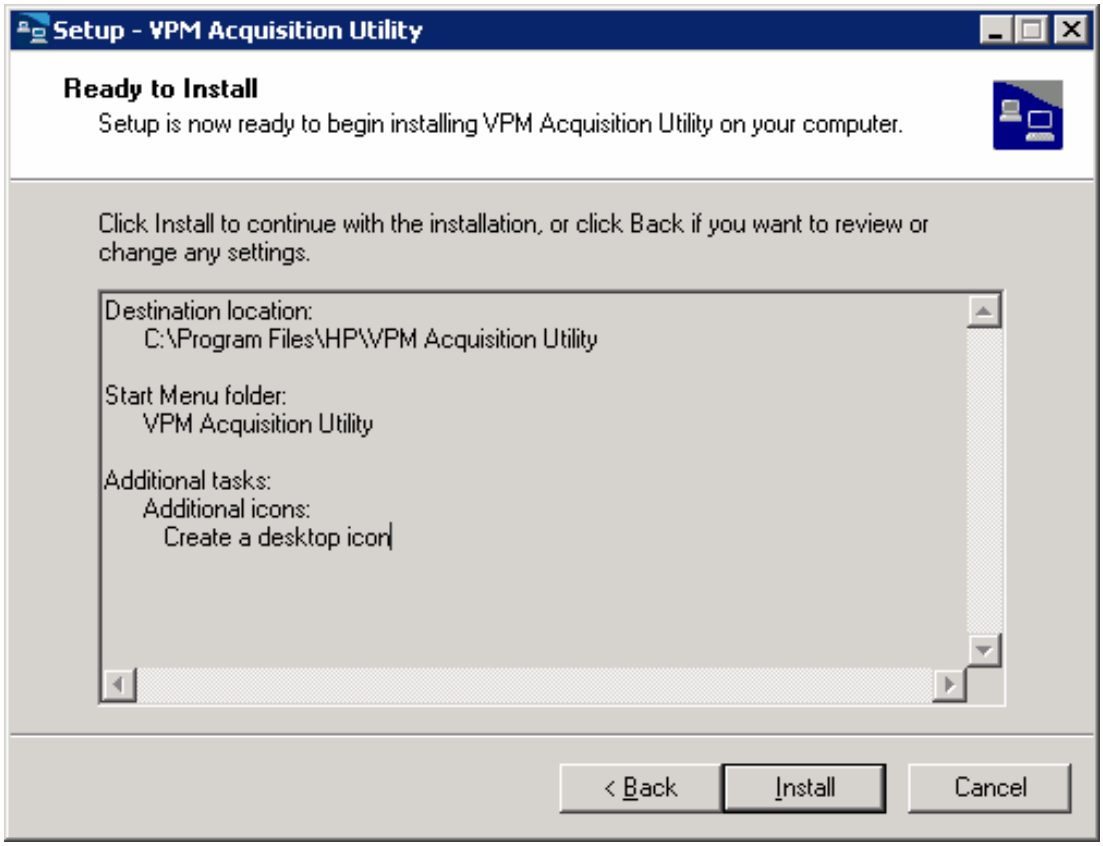
8. Specify the Start Menu folder or accept the default folder, and click **Next.**



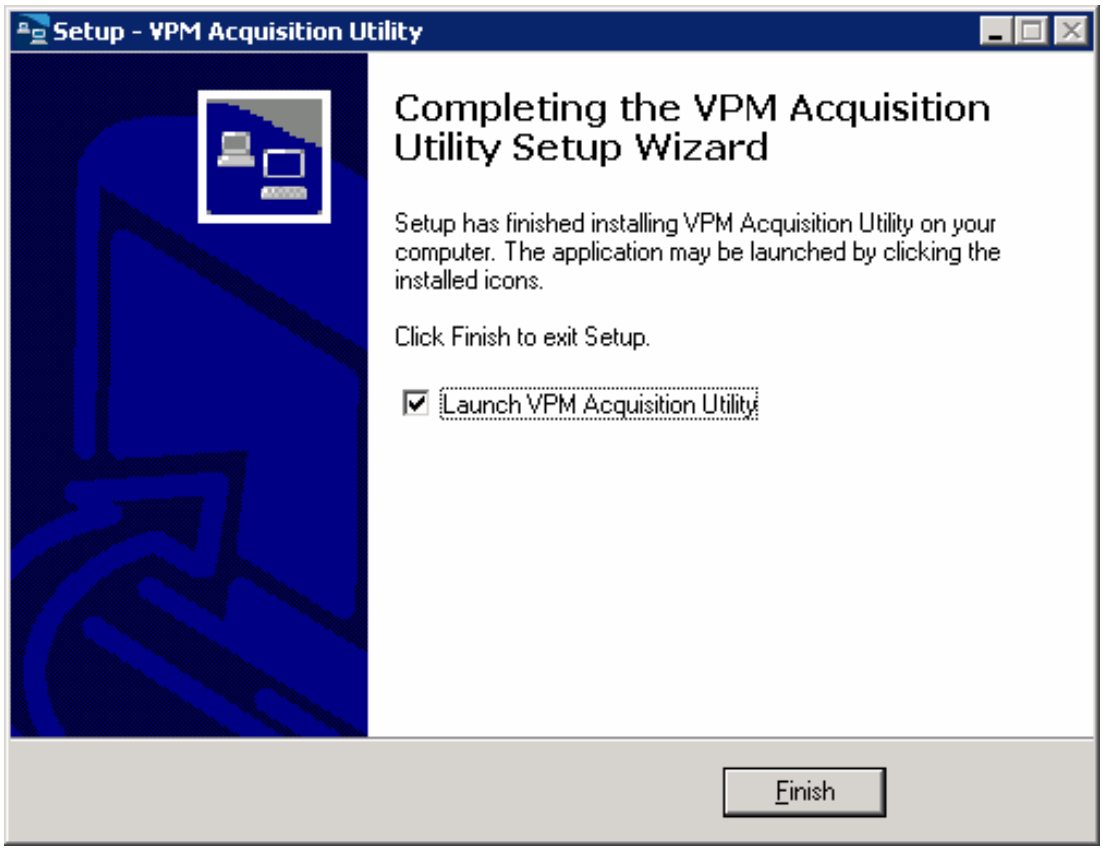
9. Select whether to create a desktop icon and quick launch icon for the VPM Acquisition Utility, and click **Next.**



10. Review the installation details. Click **Back** to change any settings, or click **Install** to begin the installation.



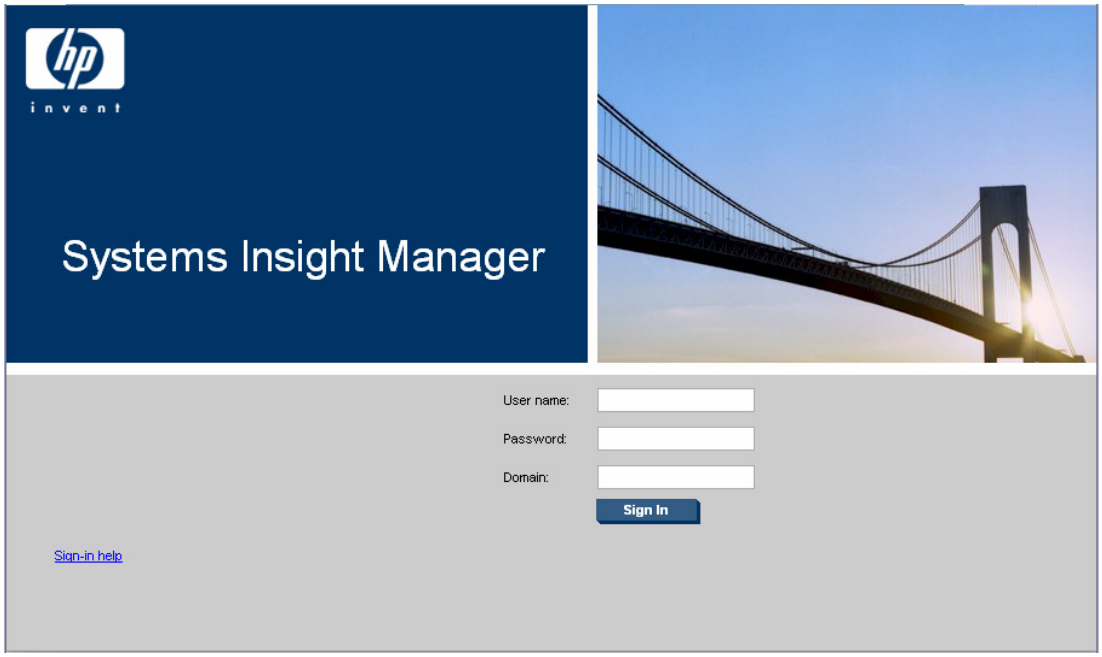
11. When the installation is complete, select whether to launch the VPM Acquisition Utility, and click **Finish.**



Post-installation configuration

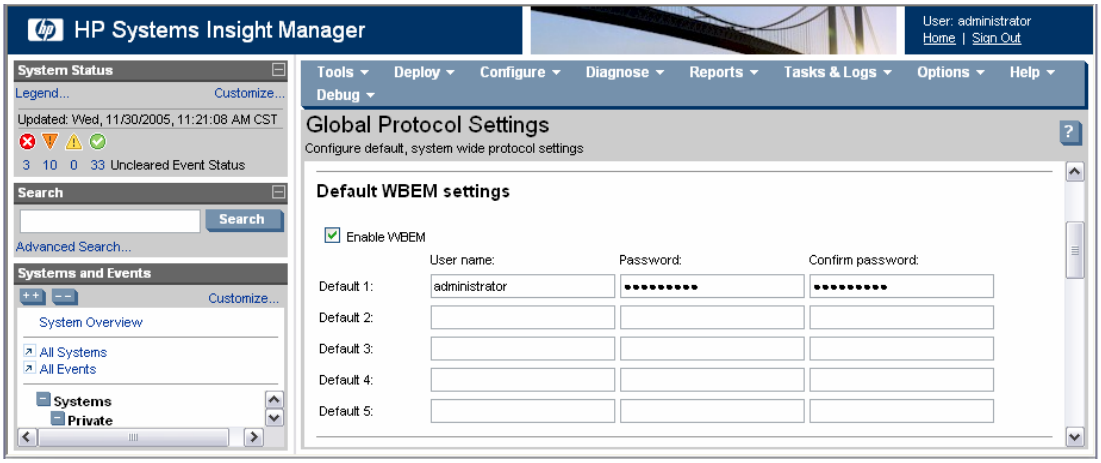
1. Log in to HP SIM from an account with administrator privileges.

NOTE: An administrator can add new users and set up existing users to access Vulnerability and Patch Management Pack. For instructions, see the *HP Systems Insight Manager Installation and Configuration Guide*.



IMPORTANT: This configuration step must be completed for Vulnerability and Patch Management Pack to function properly.

2. Select **Options>Protocol Settings>Global Protocol Settings,** and configure the WBEM credentials to enable access to target systems using one of the following options.
   - Configure settings for the \user account if Vulnerability and Patch Management Pack is located on the HP SIM server
   - Configure settings for the DOMAIN\user account if Vulnerability and Patch Management Pack is on a separate server.
3. Enter the Windows administrator account credentials in the Default 1 field and Red Hat administrator group credentials in the Default 2 field. For systems with individual settings, configure WBEM credentials using the System Protocol Settings. For information, see the "Troubleshooting" section.
4. Click **OK**.



5. Perform an automatic discovery to locate and identify target systems in the network that can be used with Vulnerability and Patch Management Pack. For information about performing a discovery and other basic HP SIM tasks, see the *HP Systems Insight Manager Installation and Configuration Guide.*

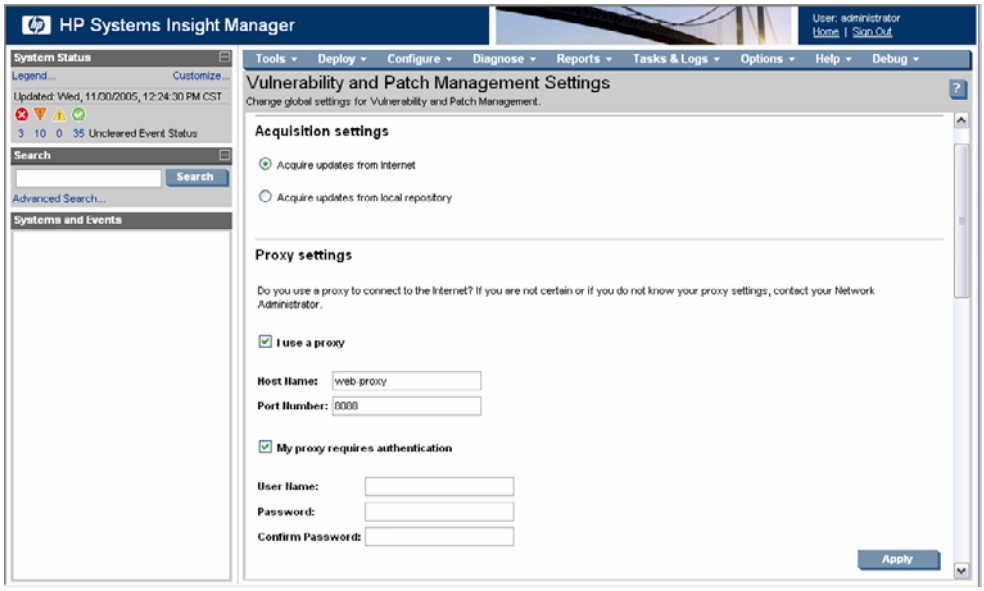
Establishing security

HP recommends the following actions to ensure security on the VPM and HP SIM servers:

- Restrict the number of local users
- Restrict or remove remote users
- Enable high security measures, such as audit logging and enhanced password restrictions
- Remove remote shares when possible

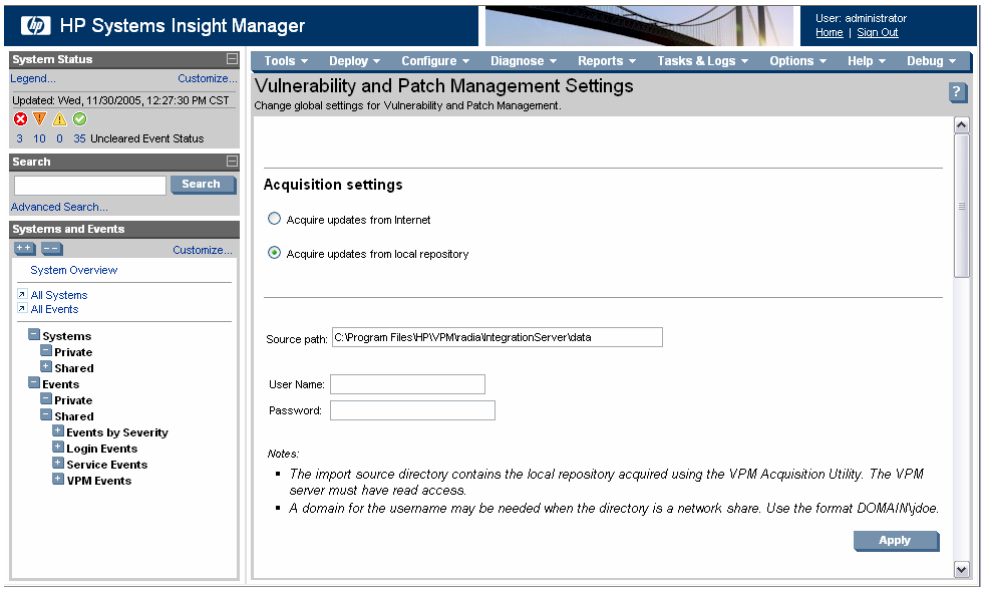
Modifying the Vulnerability and Patch Management Pack settings

1. Select **Options>Vulnerability and Patch Management>Settings.**
2. Select the source where patch and vulnerability updates will be obtained.
   - If the VPM server has direct Internet access, select **Acquire updates from Internet** to use the VPM server to obtain updates. If you use a proxy server, select the appropriate checkbox, and enter your configuration information. If the proxy requires authentication, select the appropriate checkbox, and enter your user credentials. Only basic (not encrypted) authentication is supported.



- If the VPM server does not have Internet access, select **Acquire updates from local repository** to use the VPM Acquisition Utility on another system with Internet access to acquire updates. The update files can either be manually relocated to the VPM server or accessed from the network. Designate the directory path where the update files will be located in the Source path field. If necessary, enter user credentials to access the designated directory. The VPM server must have read access to the designated directory.

IMPORTANT: A patch acquisition must have already been run using the VPM Acquisition Utility and saved to the designated directory before this step can be completed successfully. For information, see the "Acquisitions using the VPM Acquisition Utility" section.



3. Click **Apply.**

Configuring Vulnerability and Patch Management Pack acquisition for Red Hat Enterprise Linux

If Red Hat patch acquisitions will be run, configure Red Hat Enterprise Linux acquisition settings:

1. Verify the Red Hat library, compat-libstdc++, is installed on all Red Hat target systems.
2. Verify that each Red Hat target system to be patched has a valid subscription and license for the Red Hat Network, which are required for patch acquisitions. For information about subscribing to the Red Hat Network, see **http://www.redhat.com**.
3. Log in to a Red Hat Enterprise Linux 2.1, 3, or 4 server as `root`.
4. Execute the following command: `rhn_register`
5. Select **Existing,** and enter your user credentials.
6. Enter a unique profile name for this machine (such as the IP address or host name).
7. Exit the rhn_register application without applying any patches to the system.
8. Copy the file created by the rhn_register tool from /etc/sysconfig/rhn/systemid to C:\Program Files\HP\VPM\radia\IntegrationServer\etc.
9. Rename the systemid file to reflect the appropriate Red Hat distribution.
   - If the system that created the systemid file was running Red Hat Enterprise Linux 4 ES, rename the file "redhat-4es.sid."
   - If the system that created the systemid file was running Red Hat Enterprise Linux 3 ES, rename the file "redhat-3es.sid."
   - If the system that created the systemid file was running Red Hat Enterprise Linux 2.1 ES, rename the file "redhat-2.1es.sid."
   - If the system that created the systemid file was running Red Hat Enterprise Linux 4 AS, rename the file "redhat-4as.sid."
   - If the system that created the systemid file was running Red Hat Enterprise Linux 3 AS, rename the file "redhat-3as.sid."
   - If the system that created the systemid file was running Red Hat Enterprise Linux 2.1 AS, rename the file "redhat-2.1as.sid."

Acquiring Vulnerability and Patch Management Pack updates

Vulnerability and Patch Management Pack provides an acquisition utility that connects to the selected vendor website, downloads patch information and patch files, and places this information in the Vulnerability and Patch Management Pack database. Acquisitions can be run either from the VPM server in situations where the VPM server has direct access to the Internet or using the VPM Acquisition Utility installed on another system.

After Vulnerability and Patch Management Pack is installed for the first time, complete a patch acquisition to update the information in the Vulnerability and Patch Management Pack database. Also, perform patch acquisitions on a regular basis to obtain new vulnerability scan definitions and patches, ensuring that Vulnerability and Patch Management Pack is always up to date with the latest security information.

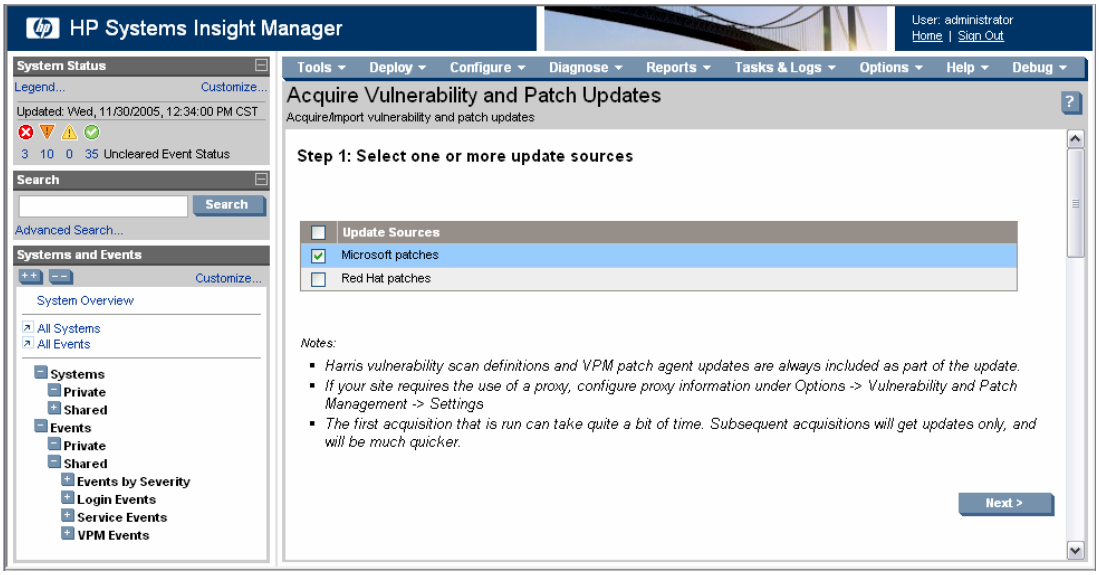
Acquisitions from the VPM server

IMPORTANT: If a proxy is used to connect to the Internet, proxy settings must be configured to acquire updates. For information, see the "Modifying the Vulnerability and Patch Management Pack settings" section.

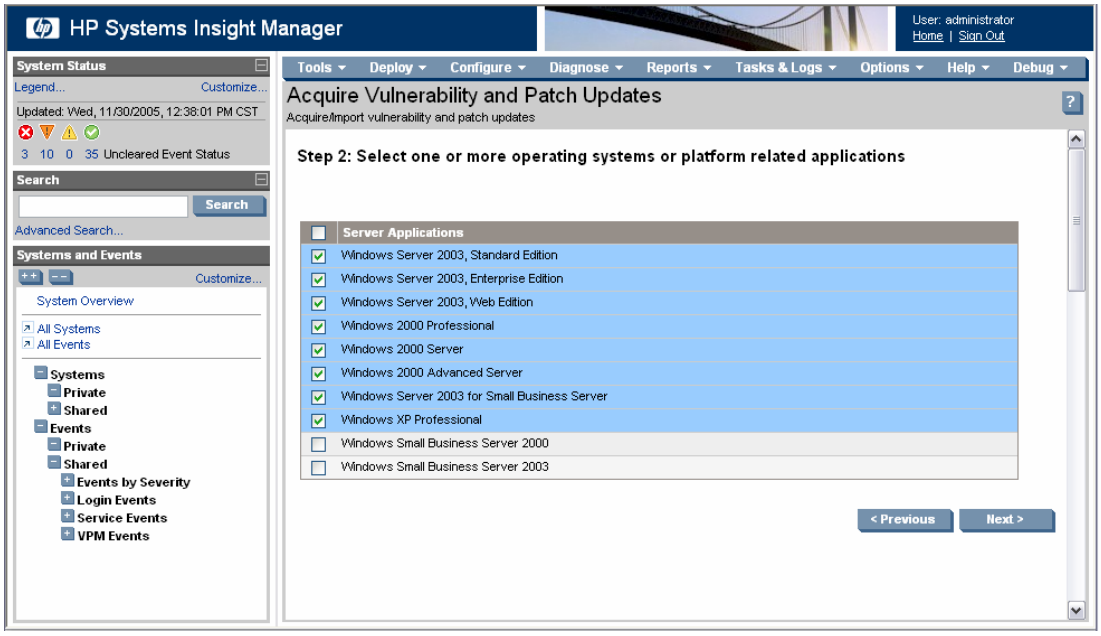
IMPORTANT: Do not schedule patch acquisition tasks to run while vulnerability scans are running. Patch acquisition tasks cause vulnerability scans to abort.

1. Select **Options>Vulnerability and Patch Management>Acquire Updates.**
2. Select one or more sources from which to acquire patch updates, and click **Next.**

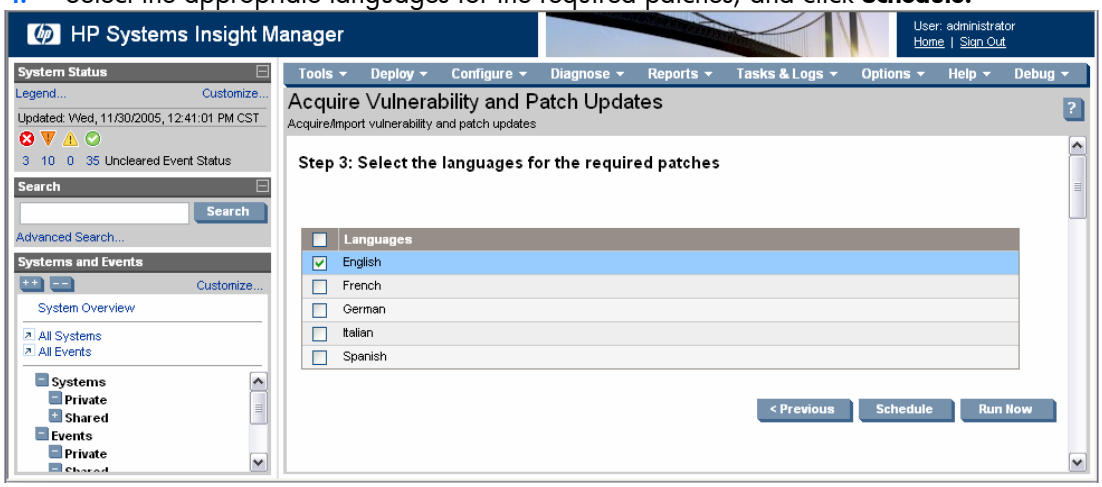
NOTE: HP updates and vulnerability scan definition files are always automatically downloaded.



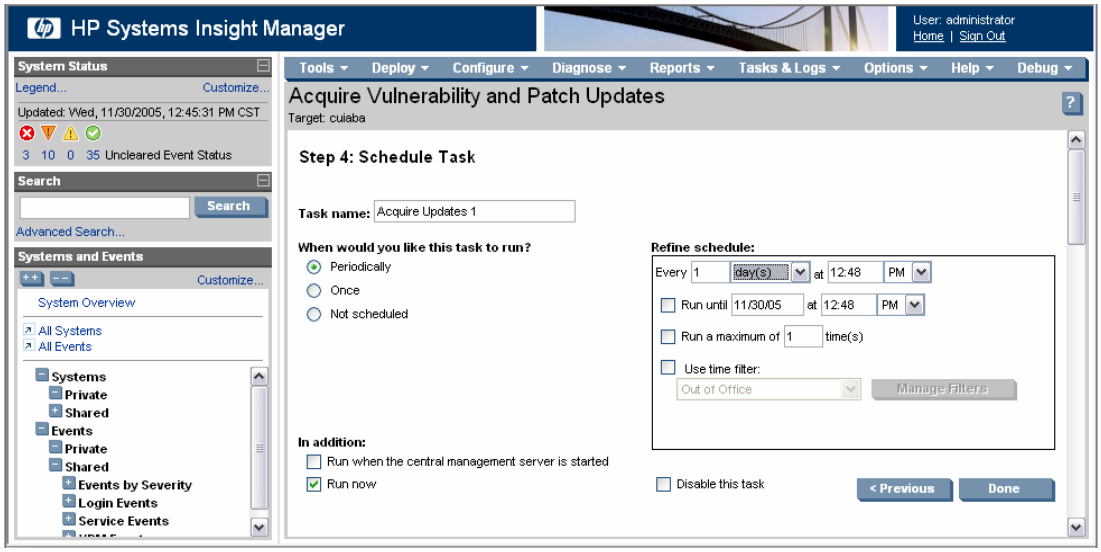
3. Select the appropriate operating systems or platforms and platform related applications, and click **Next.**



4. Select the appropriate languages for the required patches, and click **Schedule.**



5. Schedule a suitable time to acquire daily Vulnerability and Patch Management Pack updates. Updates might not be available daily, but scheduling the event daily ensures that critical updates are obtained promptly. Updates to scan definitions usually follow a few days after new patches are released.
6. Select the **Run now** checkbox to run the initial patch acquisition, and click **Done.** The first update process after the initial software installation can take up to 15 minutes or longer, depending on the number of patch sources selected and the quantity of updates available from each source.



Progress of the acquisition can be monitored at C:\Program Files\HP\VPM\Radia\IntegrationServer\logs\patch-acquire.log.

NOTE: The acquisition event might contain raw HTTP error codes, which must be decoded to determine their cause. To decode HTTP error codes, see http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html or the IIS help pages located at C:\WINNT\Help\iisHelp\common on a system where IIS is installed.

Acquisitions using the VPM Acquisition Utility

The VPM Acquisition Utility can be run from any system with Internet access to download patch information and patch files from selected vendor websites. This information can then be imported to the VPM server in the Vulnerability and Patch Management Pack database.

To run the acquisition tool, the VPM Acquisition Utility must be installed on the selected system. To install this component, see the "Installing the VPM Acquisition Utility (optional)" section.

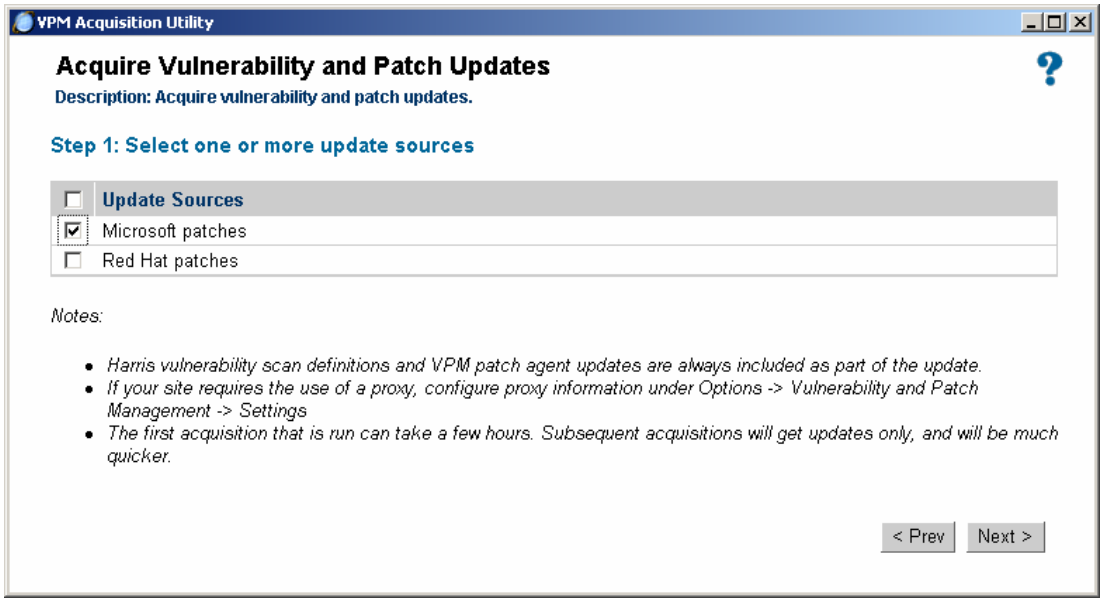
To configure and use the VPM Acquisition Utility to acquire patch and vulnerability updates:

1. Access the VPM Acquisition Utility from the selected system.
2. Select one or more sources from which to acquire patch updates, and click **Next.**

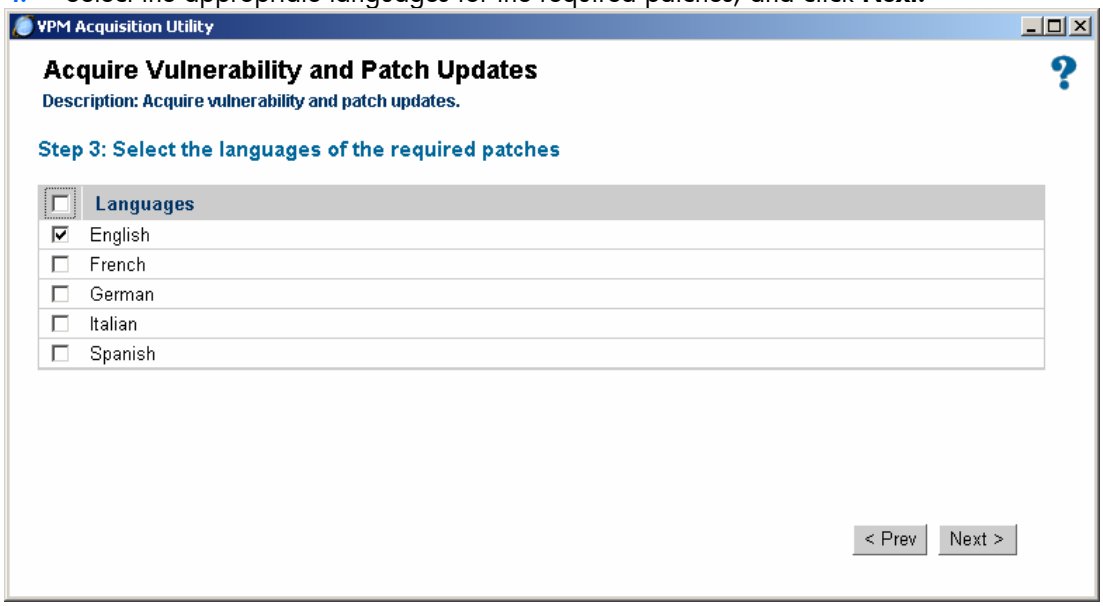
NOTE: HP updates and vulnerability scan definition files are always automatically downloaded.

NOTE: Patch acquisitions performed using the VPM Acquisition Utility cannot currently be scheduled.

NOTE: Steps 1 through 7 are only necessary the first time the VPM Acquisition Utility is used. This information is retained for future use, with the option to modify the information each time the utility is run.

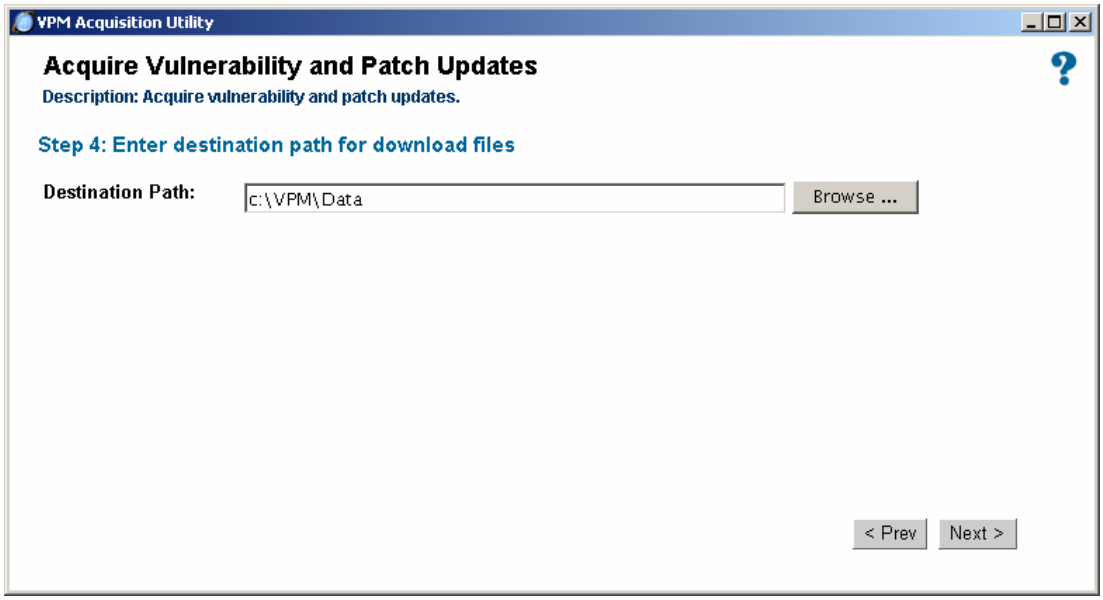


3. Select the appropriate operating system platforms and platform-related applications, and click **Next.**
4. Select the appropriate languages for the required patches, and click **Next.**

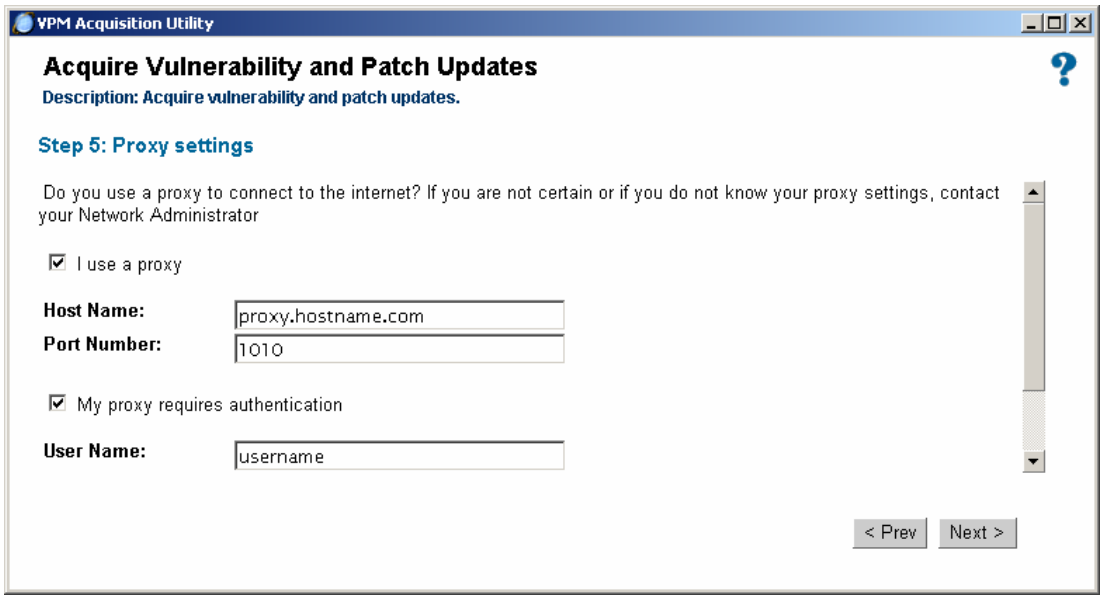


5. Enter the appropriate destination path for downloaded files, and click **Next.** The destination can be either a local or shared directory.

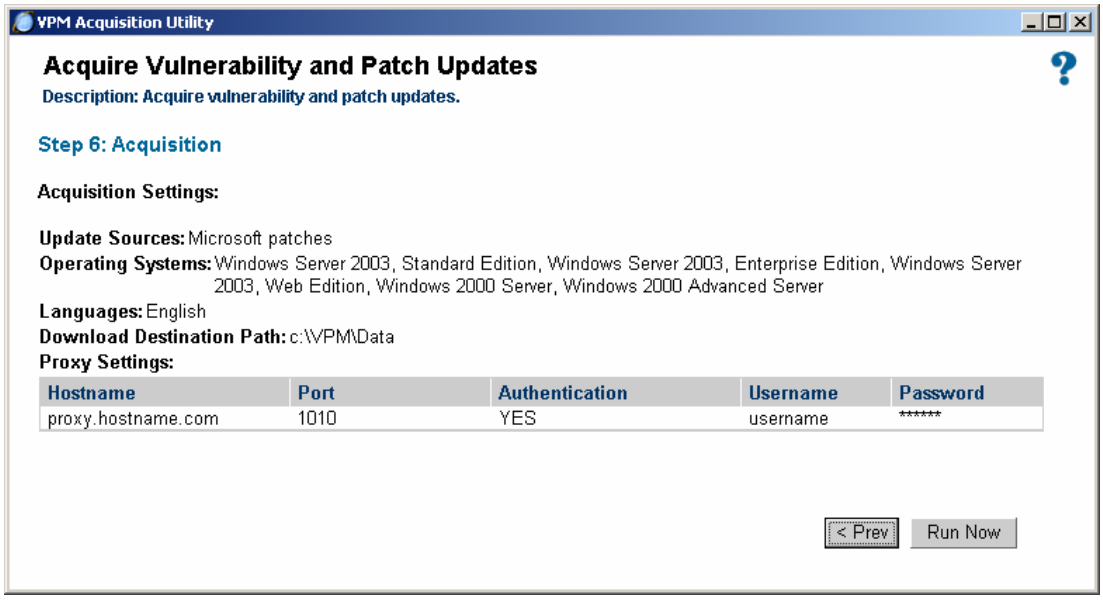
IMPORTANT: The designated directory must be accessible.



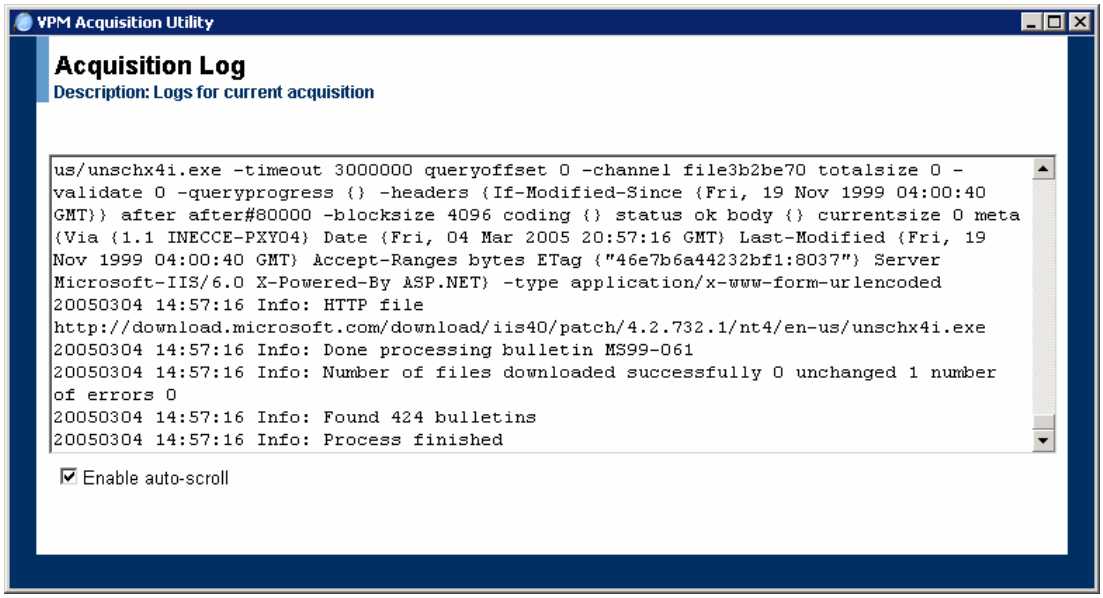
6. If you use a proxy, select the **I use a proxy** checkbox, and enter the appropriate configuration information.
7. If your proxy requires authentication, select the **My proxy requires authentication** checkbox, and enter the appropriate user credentials. Only basic (not encrypted) authentication is supported.
8. Click **Next.**



9. Click **Run Now** to run the patch acquisition.



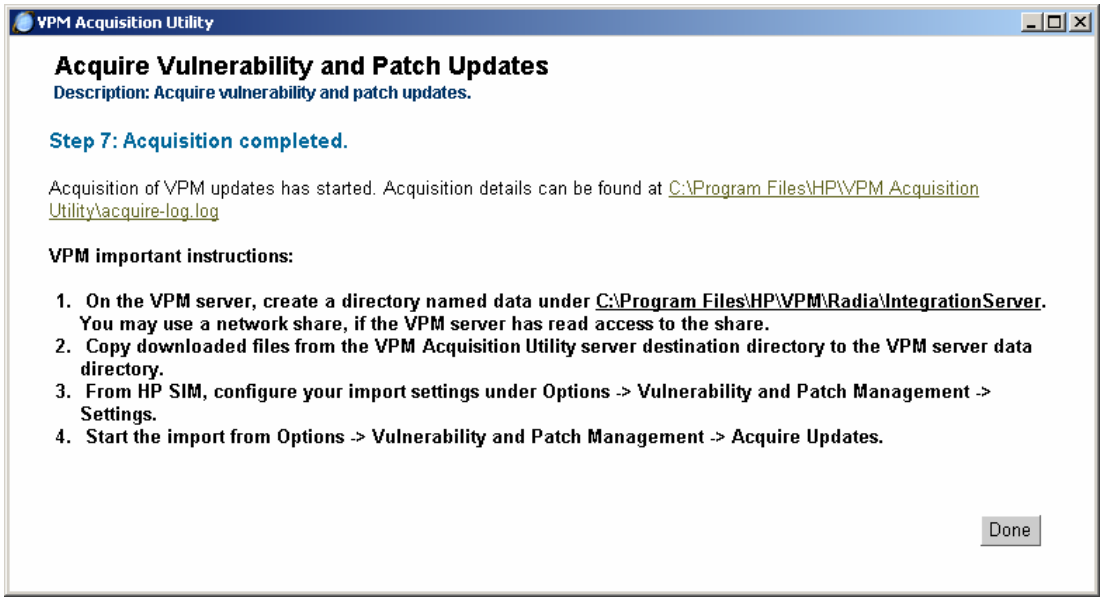
The vulnerability and patch acquisition begins. Progress of the acquisition can be monitored at C:\Program Files\HP\VPM Acquisition Utility\logs\patch-acquire.log. Clear the **Enable auto-scroll** checkbox to allow manual scrolling during the acquisition.



NOTE: The Acquisition Log is provided only to ensure that the acquisition is progressing. Disregard various messages that appear on the log screen.

NOTE: The acquisition process might appear to hang for a few moments while downloading large files.

10. Click **Done** when the acquisition process is complete.



11. On the VPM server, create a directory named “data” at C:\Program Files\HP\VPM\Radia\Integration Server. You can use a network share if the VPM server has read access to the share.
12. Copy downloaded files from the VPM Acquisition Utility server destination directory to the VPM server data directory.
13. From HP SIM, configure your import setting by selecting **Options>Vulnerability and Patch Management>Settings.**
14. Start the import process by selecting **Options>Vulnerability and Patch Management>Acquire Updates.**

Licensing

This section provides information about licensing systems for use with Vulnerability and Patch Management Pack.

NOTE: The VPM Patch Agent is automatically deployed when systems are licensed to allow patches to be applied to the systems. VPM Patch Agent updates might be acquired as part of the normal acquisition process. Agents installed on target systems are automatically updated the next time patches are applied or validated.

NOTE: A system licensed with a time-limited license key is considered an unlicensed system when the license key expires and will no longer be included in scheduled VPM tasks, such as vulnerability scans. The license status of the system appears as "Demo key expired."

Licensing within Vulnerability and Patch Management Pack

Licenses can be added and applied within Vulnerability and Patch Management Pack as a distinct step whenever a licensed operation, such as a vulnerability scan or patch deployment, is initiated and one or more target systems selected for the operation is unlicensed or licensed with a time-limited license. You are prompted to license these systems to successfully complete the requested action.

The number of available licenses and the number of selected target systems not licensed or licensed with a time-limited license appear. To apply licenses to these target systems:

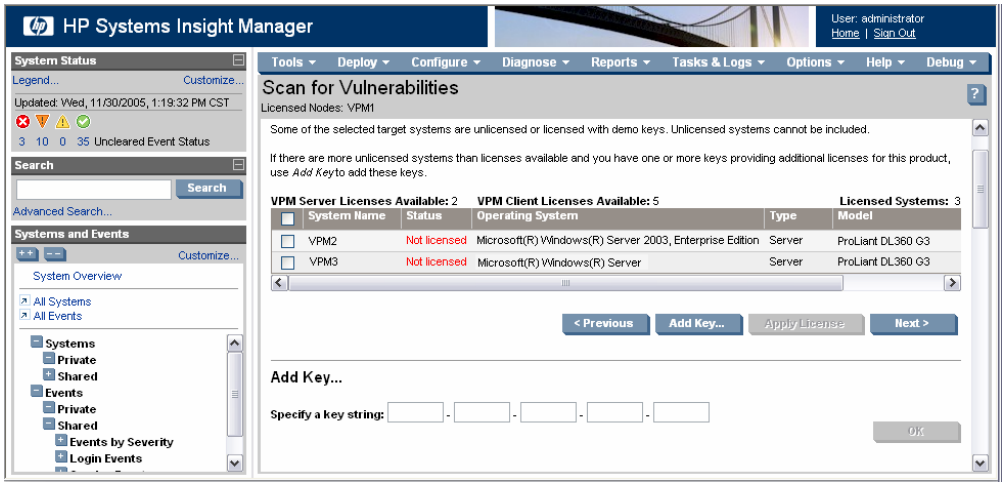
1. If licenses are available, select any unlicensed system in the list to license, not exceeding the number of available licenses, and click **Apply License.** Licenses are automatically applied to the appropriate systems.

IMPORTANT: If systems listed as Unknown or Unmanaged in HP SIM are selected for licensing, a server license is assumed and automatically applied. HP recommends modifying the HP SIM settings to properly identify systems before licensing.

IMPORTANT: Any unlicensed systems not licensed at this time will not be included in the task.

NOTE: The Apply License button is only enabled if sufficient licenses are available to license the selected systems.

2. If you have additional licenses, click **Add Key** to enter one or more new key strings, which can be cut and pasted as one string into any one of the subfields, and click **OK.**



3. Click **Next** to continue the task.

NOTE: Selected target systems not yet licensed or licensed using a time-limited license appear in the systems list on the license validation page. This page reappears, displaying the updated licensing status, each time a license is added or applied to a system. Time-limited licenses can be changed to permanent licenses at this time by selecting the node and applying a permanent license. When all selected target systems are licensed, the process moves to the next step of the selected operation. If all target systems initially selected for the task are licensed with permanent licenses, the license validation page does not appear.

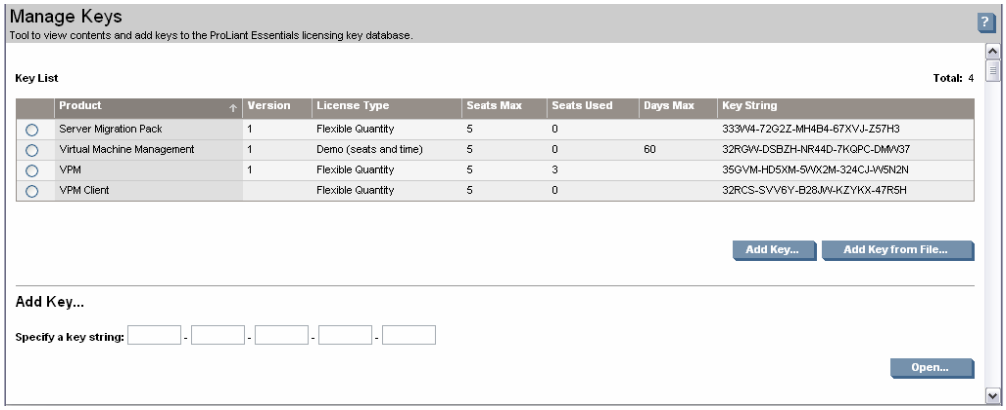
Licensing using the HP SIM License Manager

The HP SIM License Manager can be used to manage licenses. All license keys seen by the License Manager appear when the function starts, as well as the key details and summary status. Select any key and a new table appears. Systems assigned to that key, details about the system, and the status of the key on that system appear.

Adding licenses

The HP SIM License Manager can be used to add Vulnerability and Patch Management Pack licenses to the licensing database.

1. Select **Deploy>License Manager>Manage Keys.**
2. Click **Add Key** to enter one or more new key strings, which can be cut and pasted as one string into any of the subfields.
3. Click **Open.**



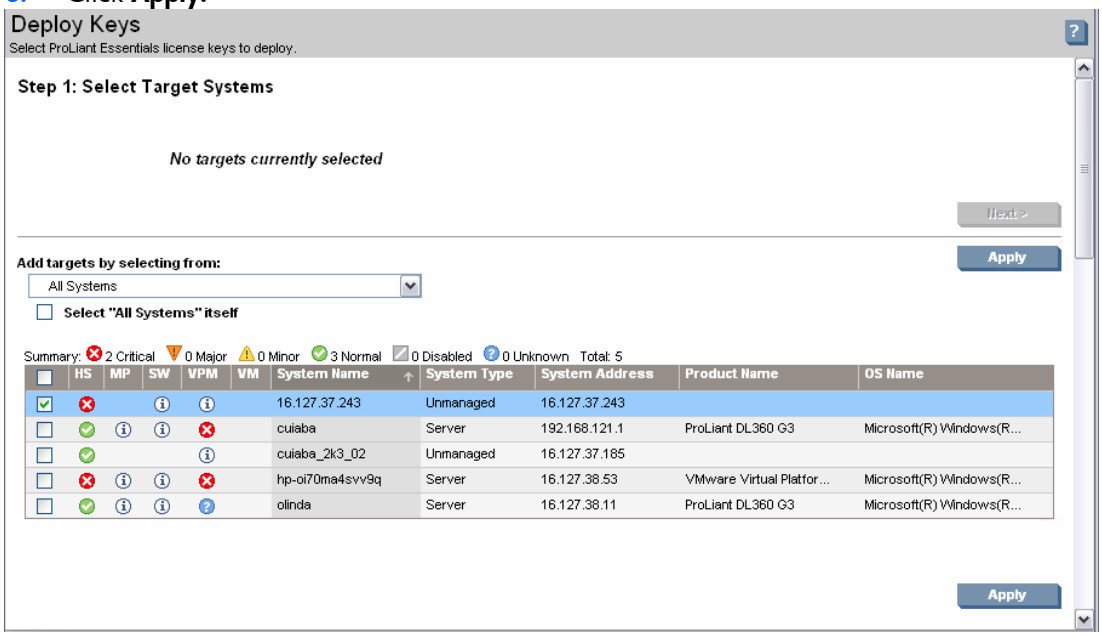
NOTE: Vulnerability and Patch Management Pack does not support the HP SIM License Manager Add Key from File feature.

NOTE: If the license key is not valid or is a duplicate of a key already existing in the database, an error message appears, and the license key is not added to the database.

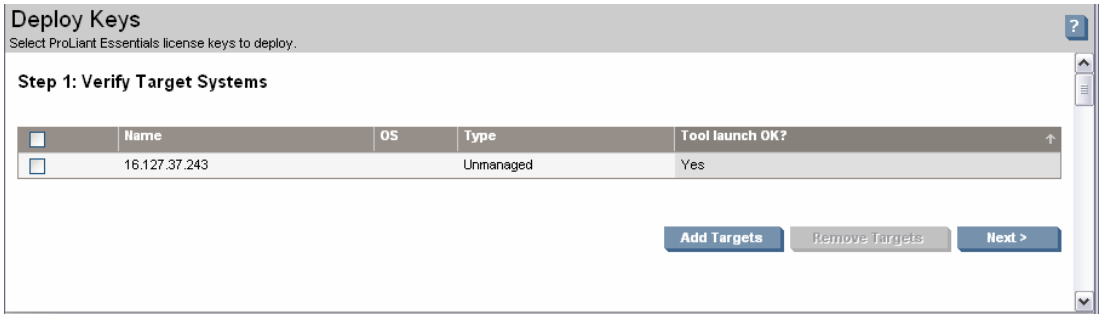
Applying licenses to selected systems

To apply licenses to target systems:

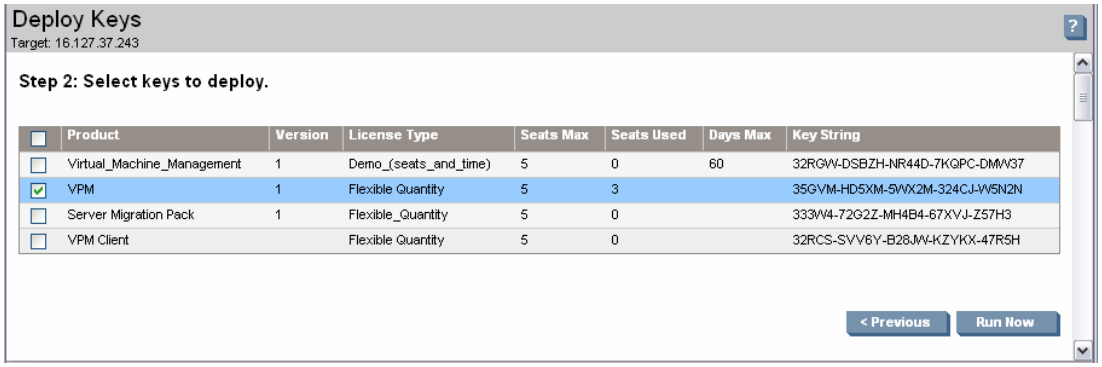
1. Select **Deploy>License Manager>Deploy Keys.**
2. Select the target systems to license either by selecting a group from the dropdown list or by selecting the checkbox next to individual systems.
3. Click **Apply.**



4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets** if it is necessary to reselect target systems, and click **Next.**



5. Select the appropriate Vulnerability and Patch Management Pack license key to apply to the selected systems.
6. Click **Run Now.**



Vulnerability scanning

This section provides an overview of setting up and using the Vulnerability and Patch Management Pack scanning functionality.

Vulnerability scanning is powered by technology from the Patchlink Corporation's STAT Scanner. Patchlink Corporation is an international communications equipment company focused on providing mission-critical assured communications for commercial and government customers.

Patchlink Corporation's STAT network security solutions are backed by decades of expertise in information security. STAT vulnerability management products provide proactive protection of information and computer networks from hackers, viruses, worms, and other threats.

Provided scan definitions

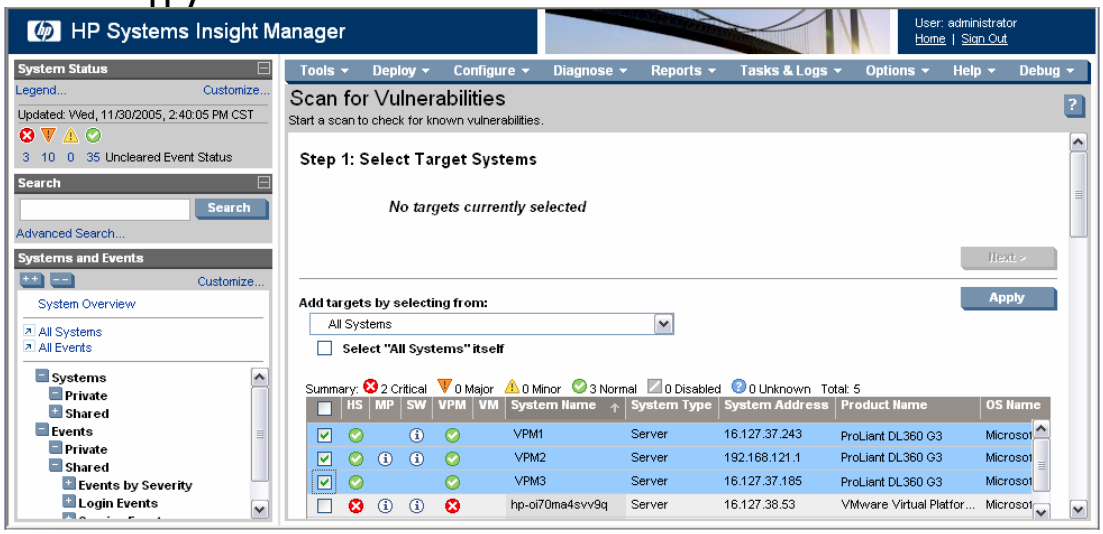
Vulnerability and Patch Management Pack provides a large variety of scan definitions. These scans can be used to search for vulnerabilities or modified to suit the specific needs of your environment. For specific information about the provided scan definitions, see the "Vulnerability and Patch Management Pack provided scan definitions" section.

To use the provided scan definitions, see the instructions in the "Scanning for vulnerabilities" section.

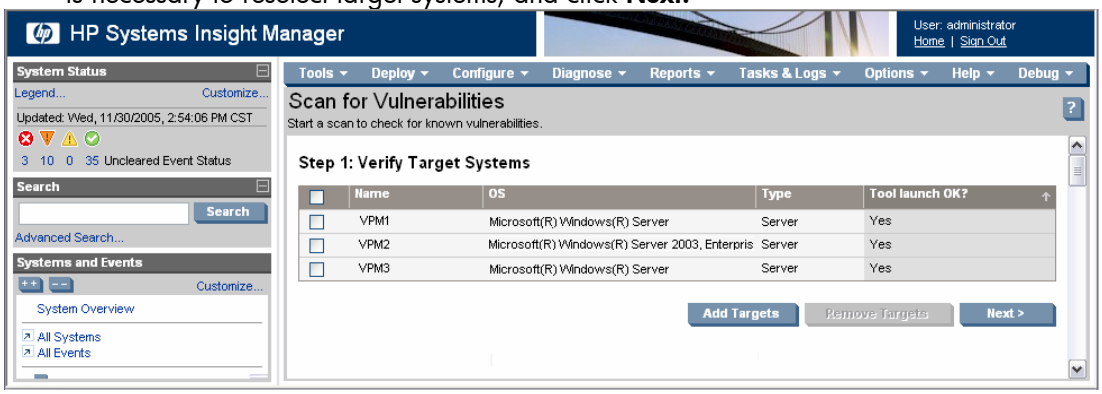
Scanning for vulnerabilities

To perform a vulnerability scan:

1. Select **Diagnose>Vulnerability and Patch Management>Scan>Scan for Vulnerabilities.**
2. Select the target systems to scan either by selecting a group from the dropdown list or by selecting the checkbox next to individual systems.
3. Click **Apply.**



4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets** if it is necessary to reselect target systems, and click **Next.**



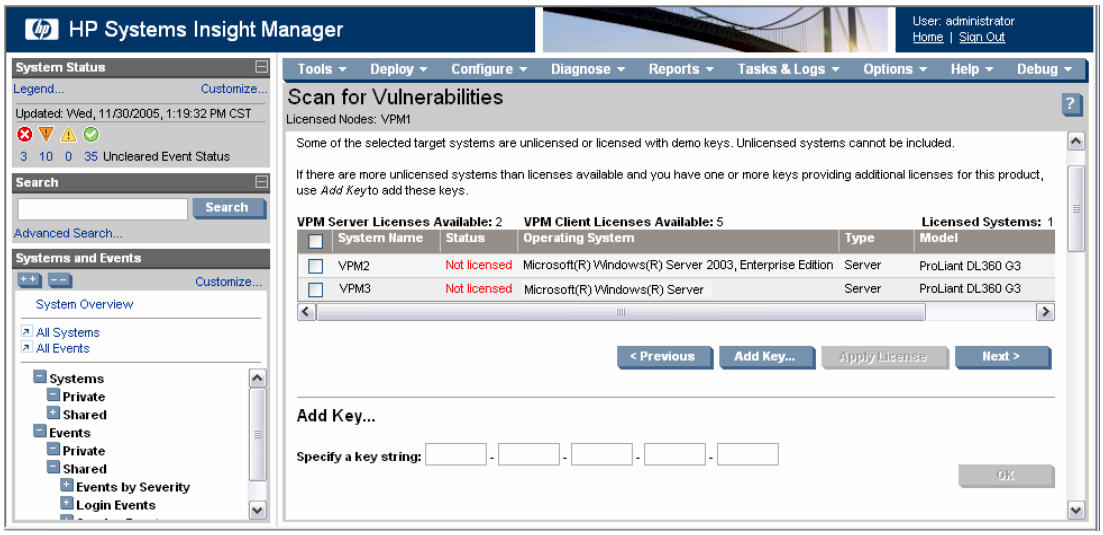
5. If any selected systems are unlicensed or licensed with a time-limited license, permanent licenses can be applied at this time. If licenses are available, select any unlicensed system in the list, and click **Apply License.** To add licenses using a key string, click **Add Key,** enter the key string in the field, and click **OK.**

IMPORTANT: If systems listed as Unknown or Unmanaged in HP SIM are selected for licensing, a server license is assumed and automatically applied. HP recommends modifying the HP SIM settings to properly identify systems before licensing.

IMPORTANT: Any unlicensed systems not licensed at this time will not be included in the vulnerability scan.

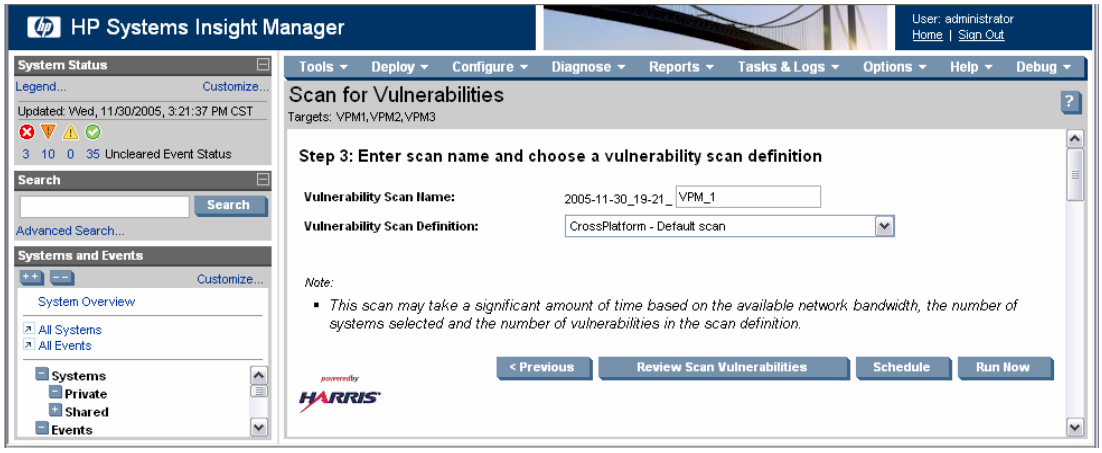
NOTE: If all target systems initially selected for the task are licensed with permanent licenses, the license validation page does not appear.

6. Click **Next.**

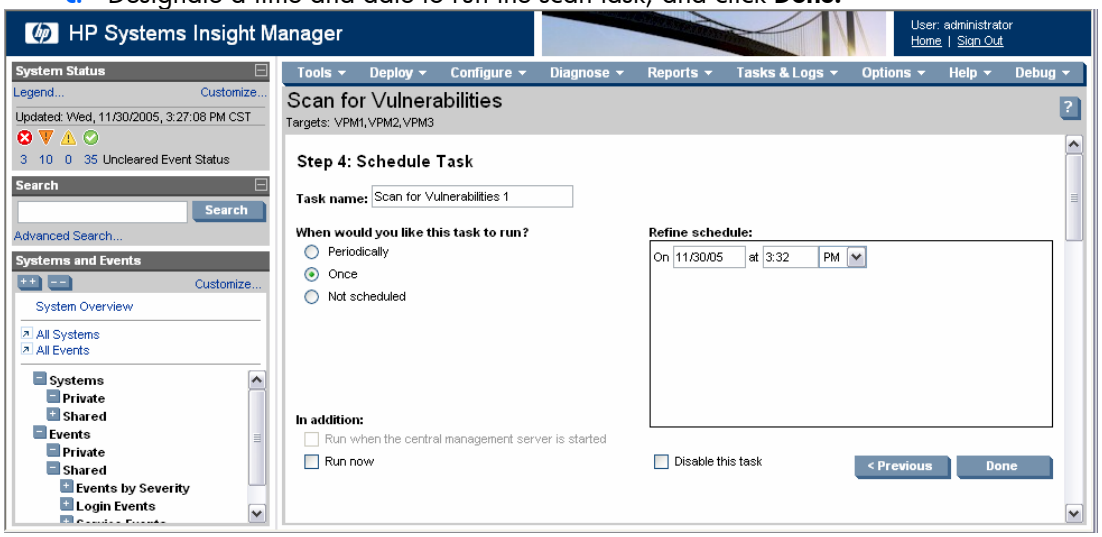


7. Enter a name for the vulnerability scan, and select a scan definition from the dropdown list.
8. To run the vulnerability scan immediately, click **Run Now.** To schedule the scan to run at a later time, select **Schedule.**

NOTE: Scans are run one system at a time in a serial process from the VPM server.



9. If scheduling the vulnerability scan:
   a. Enter an appropriate name for the scan task, or accept the default name.
   b. To schedule the vulnerability scan to run on a regular basis, select **Periodically,** or to run the scan one time, select **Once.**
   c. Designate a time and date to run the scan task, and click **Done.**

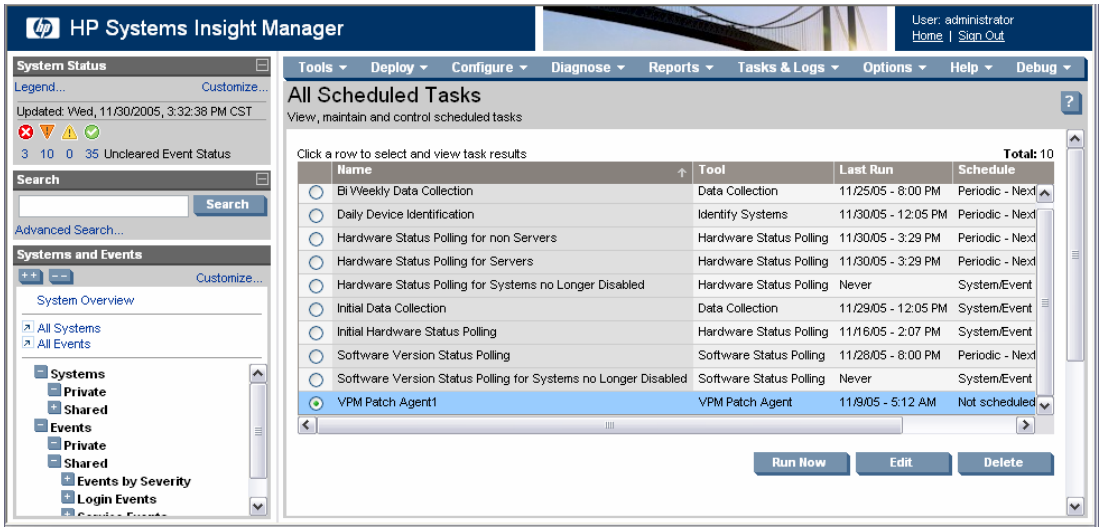


10. View scan results after the task completes either by clicking the system status icon or viewing the VPM Events list.

Viewing, modifying, or canceling a scheduled task

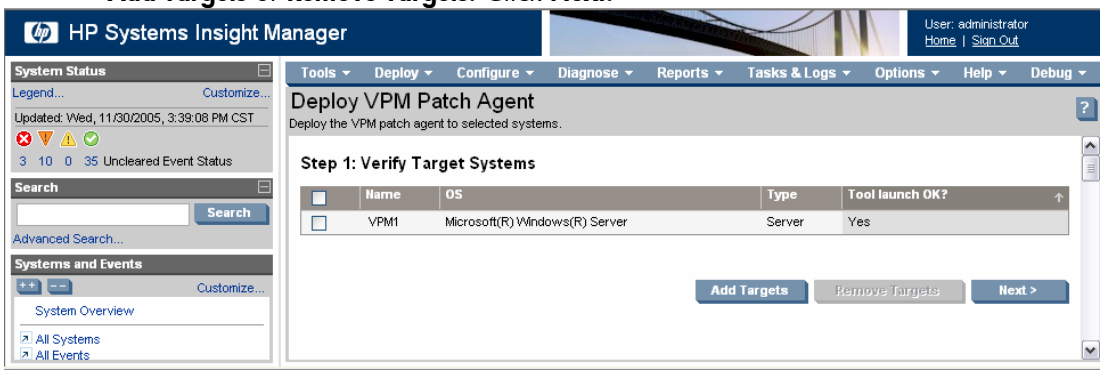
To view, modify, or cancel a task that has been previously scheduled:

1. Select **Tasks & Logs>View All Scheduled Tasks.**
2. Select the appropriate task from the list, and click **Edit.**

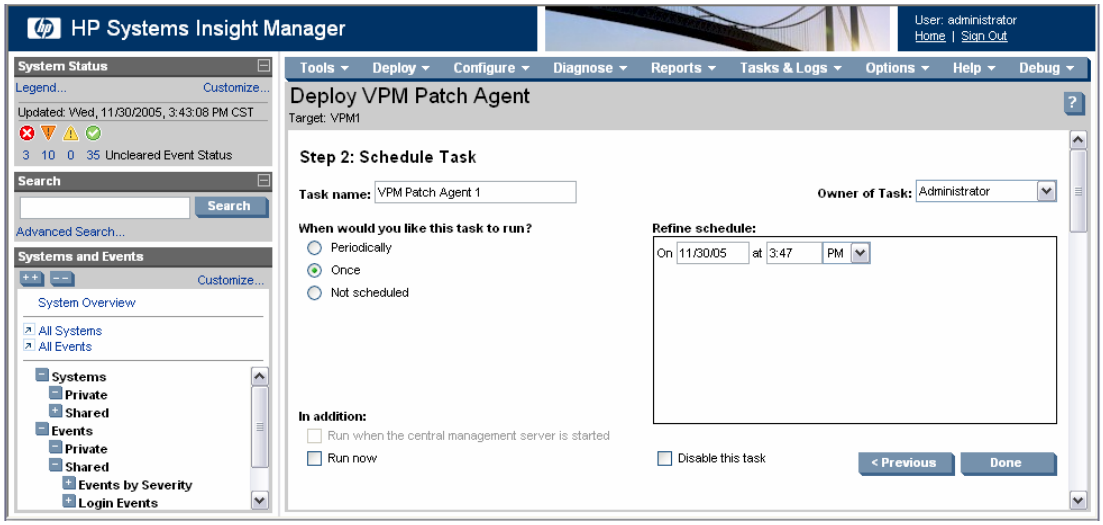


3. Modify the event details.

   a. If necessary, change target systems on which the task is scheduled to run by clicking either **Add Targets** or **Remove Targets.** Click **Next.**



   b. View the task schedule, and modify if necessary. Click **Done.**



Viewing vulnerability scan results

The Vulnerability and Patch Management Pack scan results can be viewed either for a specified vulnerability scan or for an individual system. When a vulnerability scan is run for a group of target systems, results are generated for the group as well as for each individual system. Vulnerability scan results can be viewed as .pdf files in the following formats:

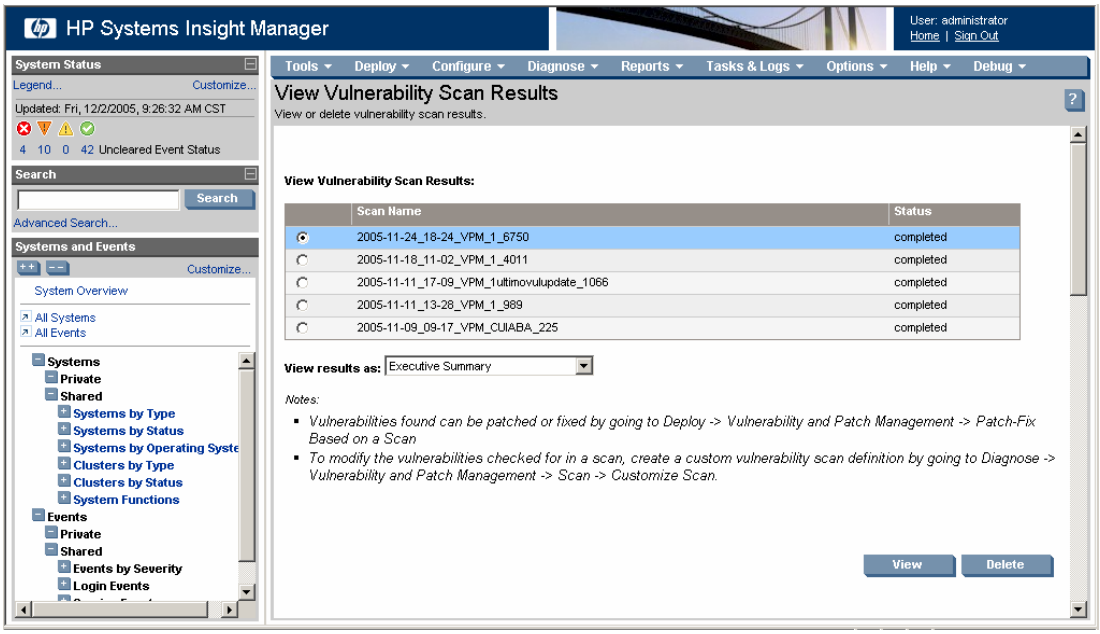
- Executive Summary—A high-level summary of all vulnerabilities found in a scan
- Detailed Listing—A list of vulnerabilities found on each system, as well as a description and risk evaluation of each
- Simple Listing—A list of vulnerabilities found on each system sorted by vulnerability name
- Scan Summary—A list of scans performed and vulnerabilities found, sorted by system name
- Ports and Services—A list of ports, services, and unknown services, sorted by system name

Vulnerability scan results guidelines

- Vulnerability scan results cannot be viewed or deleted while status displays `Scanning` or `Pending`. Vulnerability scan results for an aborted scan might not be accurate.
- If the vulnerability scan results display the message, `No file access`, verify that the WBEM settings in HP SIM have appropriate credentials listed for the target systems. For additional information, see the "Post-installation configuration" section.
- Scan results can also be accessed from the links in the completed scan event in HP SIM.
- Vulnerabilities listed are the total vulnerabilities found in the group of systems scanned. Individual systems in the group might not have every vulnerability listed.

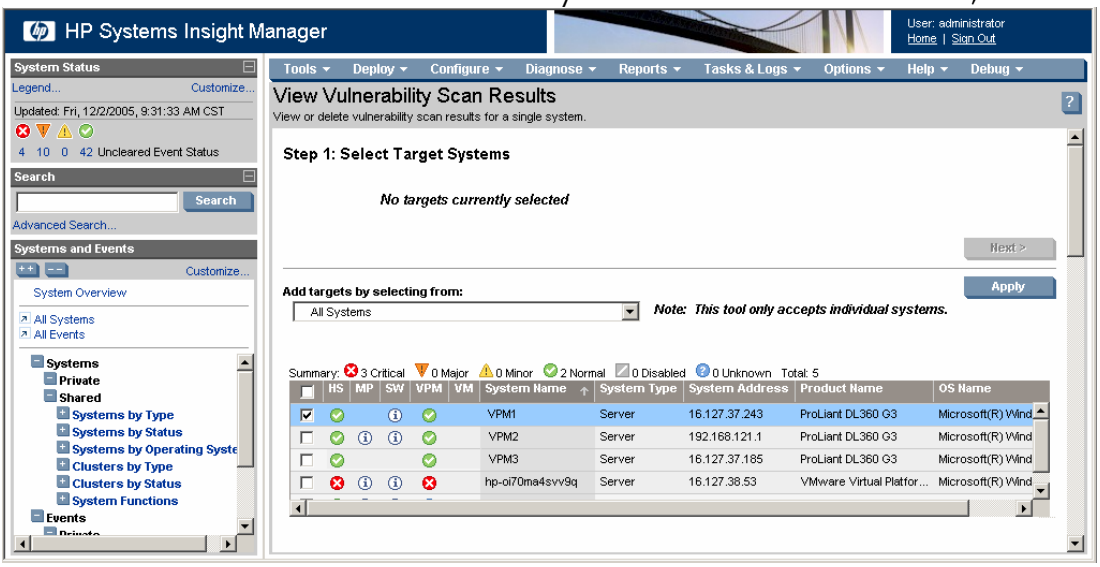
Viewing vulnerability scan results by scan name

1. Select **Diagnose>Vulnerability and Patch Management>Scan>View Results by Scan Name.**
2. Select the appropriate vulnerability scan, select the format in which to view the results from the dropdown list, and click **View.** The vulnerability scan results appear in a separate window.

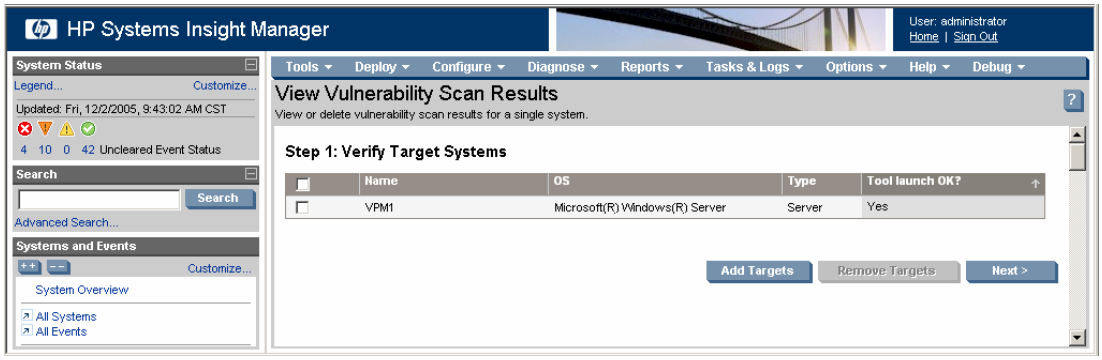


Viewing scan results by system

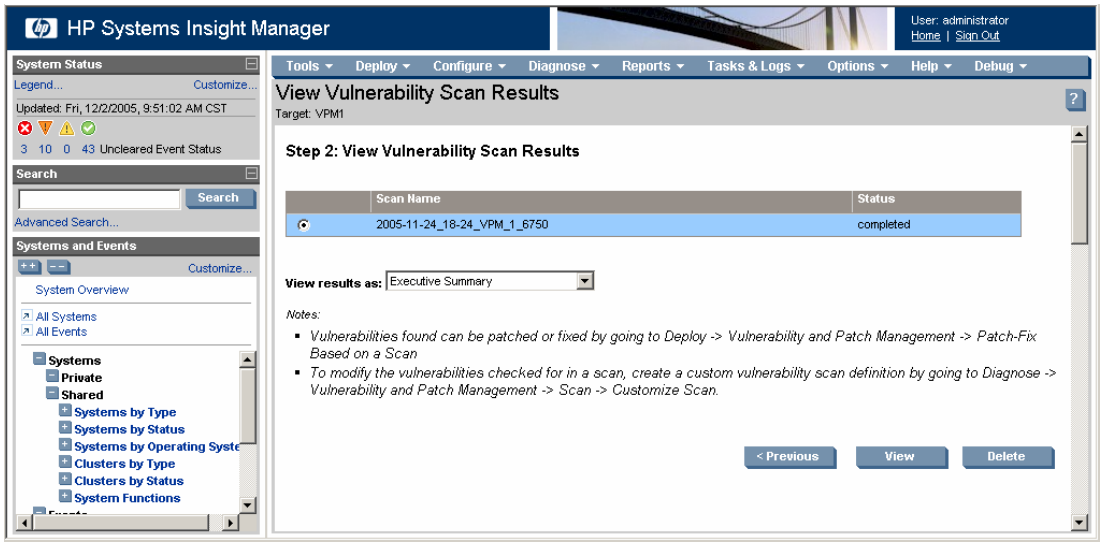
1. Select **Diagnose>Vulnerability and Patch Management>Scan>View Results by System.**
2. Select the checkbox next to the individual system for which to view scan results, and click **Apply.**



3. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets,** if necessary to reselect target systems, and click **Next.**



4. Results for all scans performed on the selected system appear. Select the scan results to view, and click **View.**

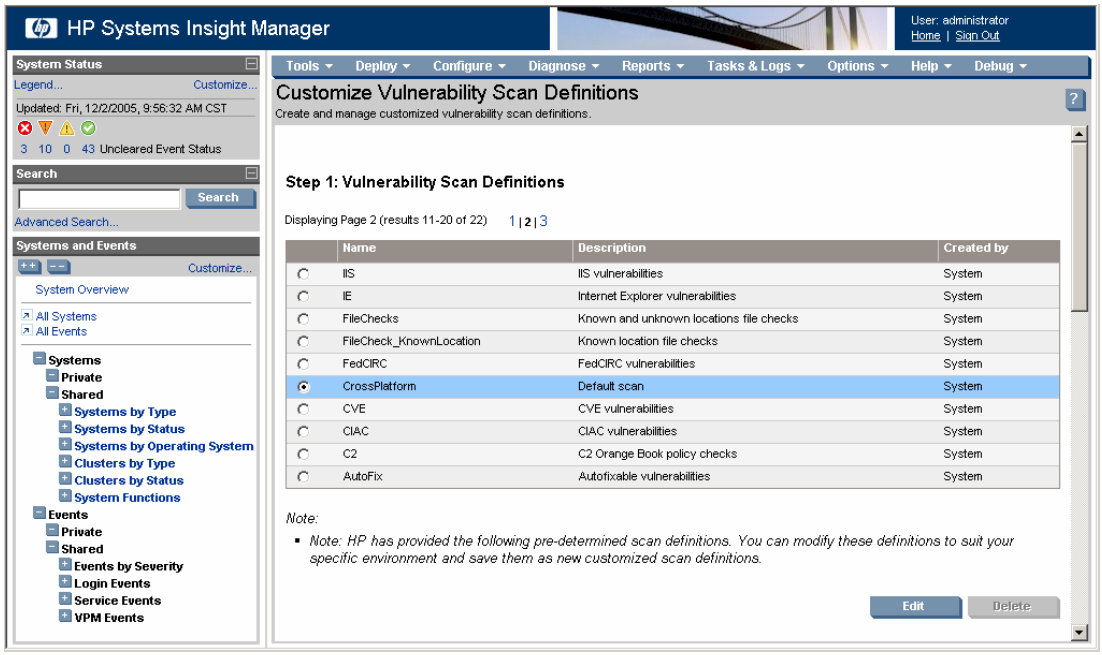


Customizing vulnerability scan definitions

NOTE: Custom scans can be created from the default system scans. When default system scans are updated, the custom scans are updated with corresponding vulnerability updates also.

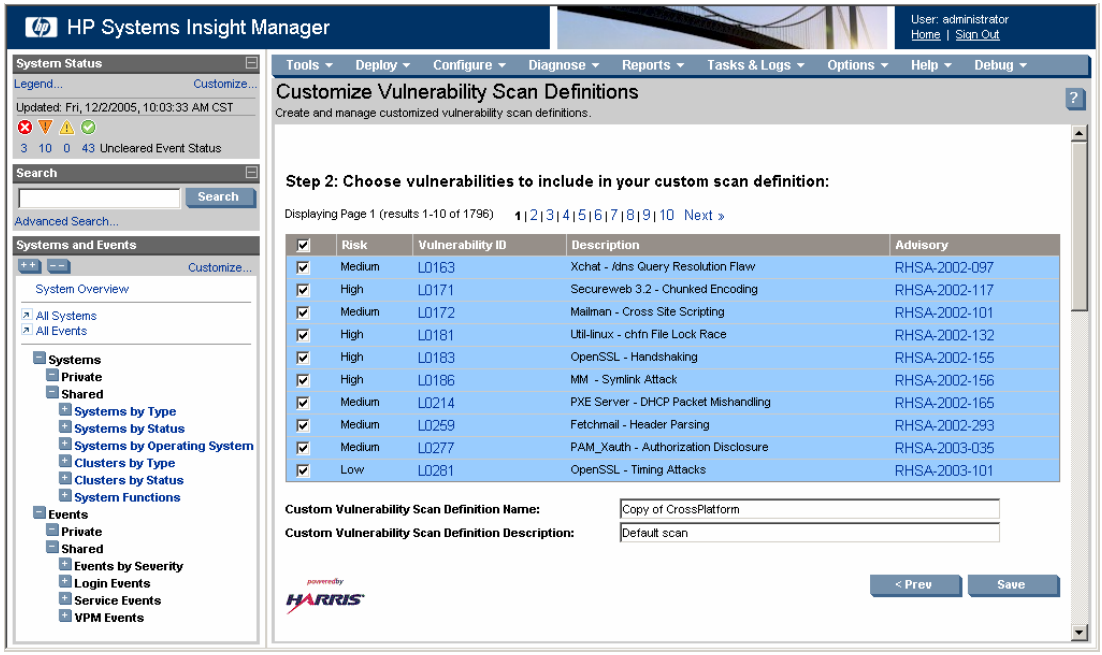
To customize the provided vulnerability scans or previously created custom vulnerability scans:

1. Select **Diagnose>Vulnerability and Patch Management>Scan>Customize Scan.**
2. Select a default system scan or a previously created vulnerability custom scan to modify, and click **Edit.** A list of vulnerabilities appears. Clicking the entry in either the Vulnerability ID or Advisory column displays additional information about the vulnerability.



3. Select one or more vulnerabilities to include in the custom scan definition.
4. Enter a name and description for the new customized vulnerability scan, and click **Save.**

IMPORTANT: The customized vulnerability scan must be renamed. The Vulnerability and Patch Management Pack default system scans cannot be modified and saved using the original scan name.



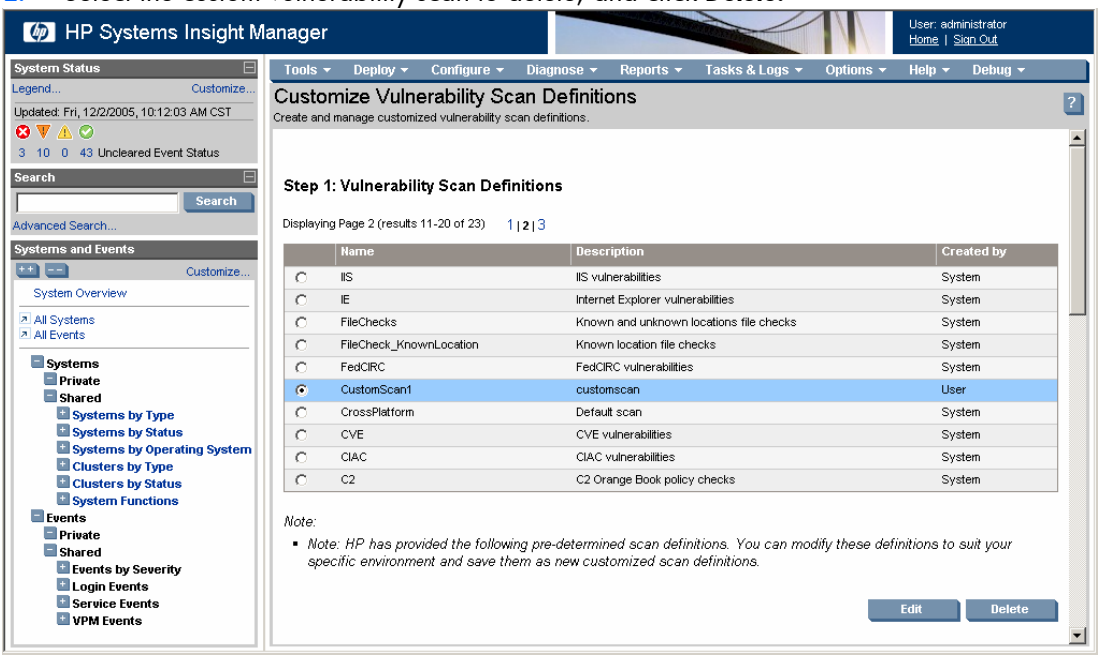
To use a customized vulnerability scan to perform scanning, see the instructions in the "Scanning for vulnerabilities" section.

Deleting a customized vulnerability scan

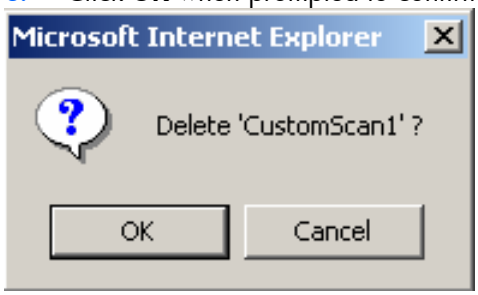
NOTE: Only custom vulnerability scans can be deleted. Default system scans provided with Vulnerability and Patch Management Pack cannot be deleted.

To delete a custom vulnerability scan:

1. Select **Diagnose>Vulnerability and Patch Management>Scan>Customize Scan.**
2. Select the custom vulnerability scan to delete, and click **Delete.**



3. Click **OK** when prompted to confirm the action.



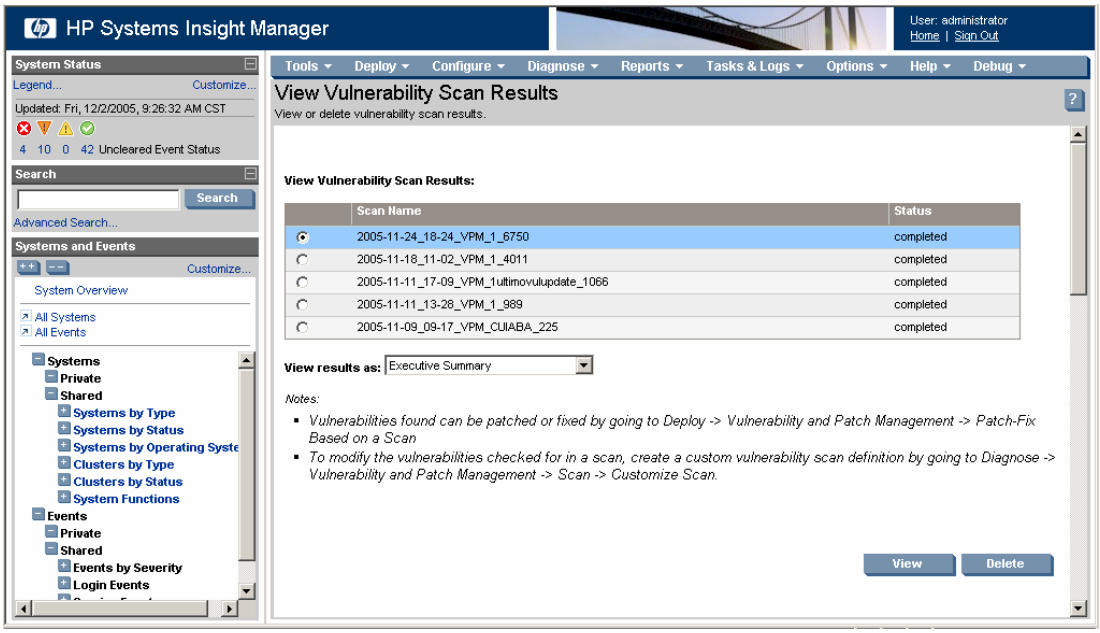
Deleting vulnerability scan results

Vulnerability and Patch Management Pack scan results can be deleted either for a specified scan or for an individual system. Removing results will break the links to the results in the events and the system list. Run another scan to create new results for the system.

Deleting scan results by scan name

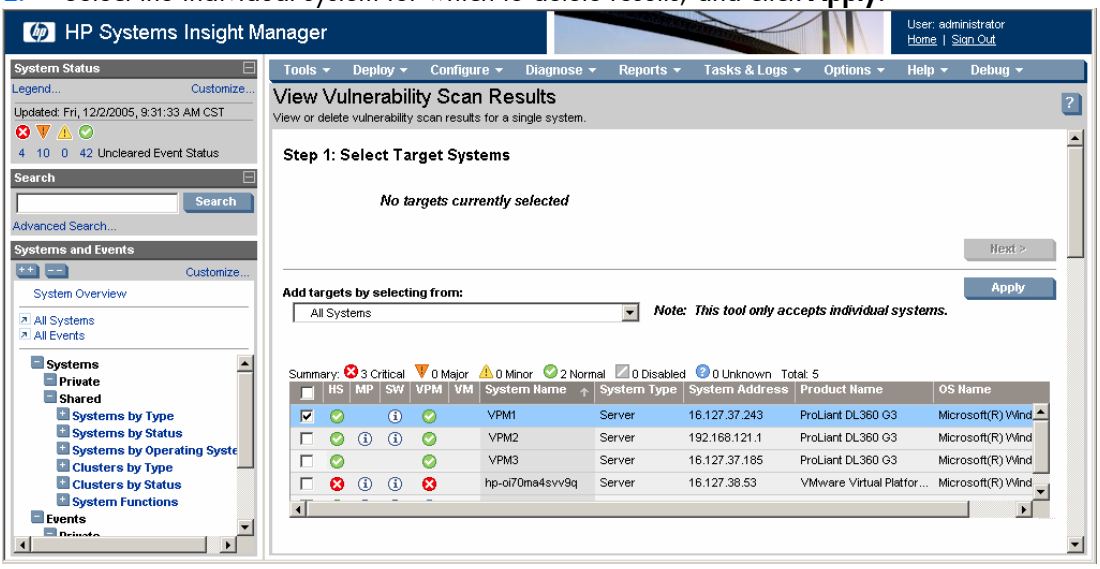
1. Select **Diagnose>Vulnerability and Patch Management>Scan>View Results by Scan Name.**

2. Select the appropriate scan or scans, and click **Delete.** All results associated with the selected scan are deleted.

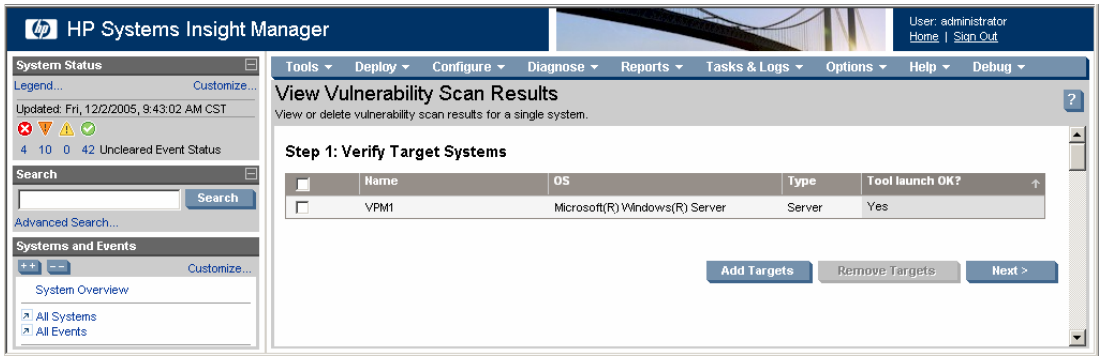


Deleting scan results by system

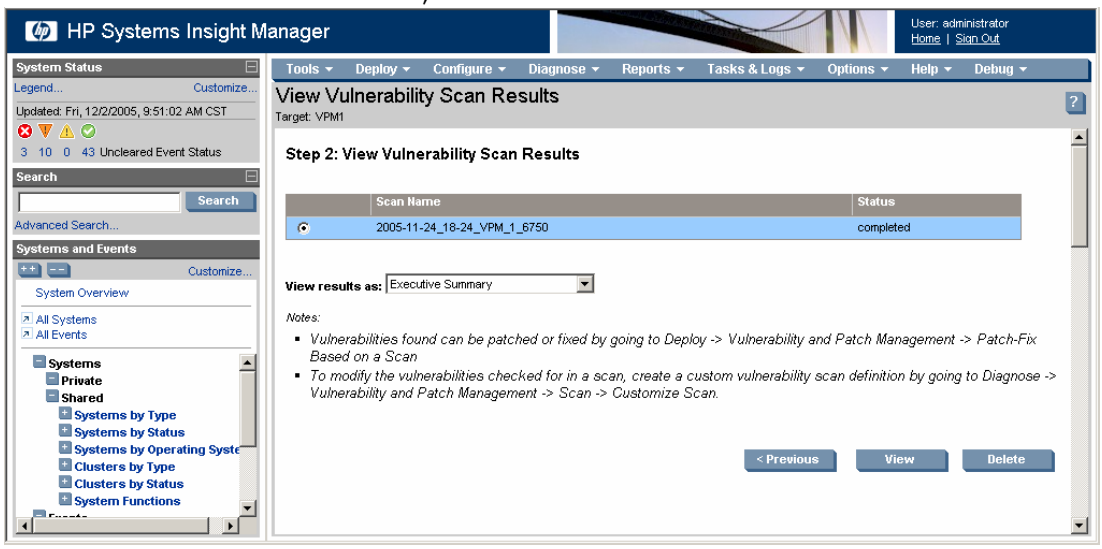
1. Select **Diagnose>Vulnerability and Patch Management>Scan>View Results by System.**
2. Select the individual system for which to delete results, and click **Apply.**



3. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets,** if necessary to reselect target systems, and click **Next.** Results from all scans performed on the selected system appear.



4. Select the scan results to delete, and click **Delete.**



Deploying patches and fixes

This section provides an overview of using Vulnerability and Patch Management Pack to deploy patches and configuration fixes.

Patches and configuration fixes can be deployed immediately or scheduled for deployment at a later time. Patches and fixes can be selected individually from the database for deployment to all systems or any combination of specified systems without performing a scan. Patches and fixes can also be deployed for all vulnerabilities identified in a particular scan.

Patches come from the software vendor and can be updated to existing software, registry, or configuration settings or files. Configuration fixes resolve incorrect system settings that can leave the system open to security threats, such as open ports or services running that are not required.

NOTE: Not all vulnerability issues found can be programmatically fixed or patched. Scan results often provide a suggested fix that must be manually performed.

Important information about patches and fixes

- Target systems are rebooted if required by the installed or removed patch, based on the reboot information obtained from the original patch source. Reboot information might occasionally inaccurately indicate whether a patch installation requires a reboot.
- If multiple patches requiring reboots are applied, target systems are only rebooted once after all patches are applied. Required reboots can be deferred and performed later. HP recommends performing required reboots as soon as possible because the status of patched systems might be unstable when a required reboot is deferred.
- To determine patch applicability, Vulnerability and Patch Management Pack might enhance patch detection criteria to be more precise than vendor information. These patches appear with an asterisk in the Patch Source column. HP does not modify the patch itself.
- Risk and Vulnerability ID information might not appear because this information was not available at the time the patch was acquired. The information appears when the vulnerability database is updated to include this information.
- By default, patches are sorted by the latest release date. Select a column heading to re-sort patches.
- Target systems that are down at the time of a scheduled patch application are patched when the system is brought online.

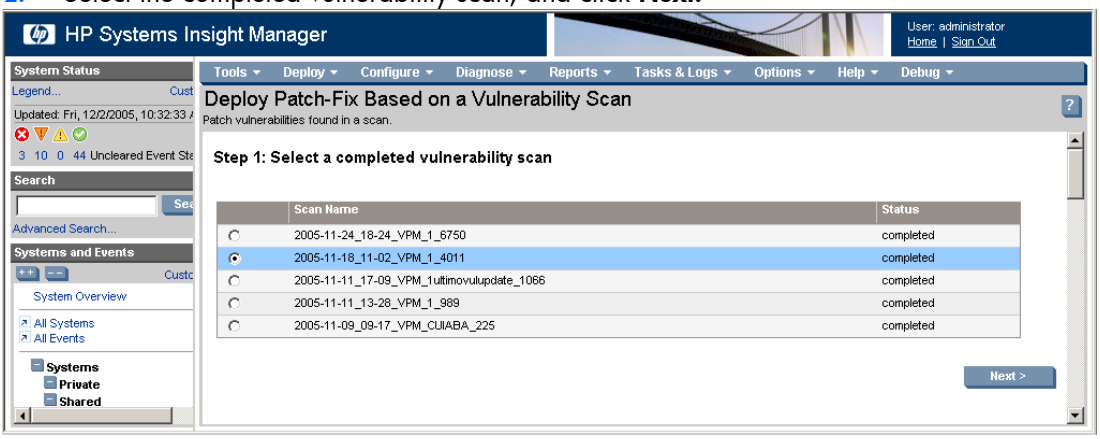
Deploying patches and fixes based on a vulnerability scan

After a vulnerability scan has been performed and it is determined that security vulnerabilities or configuration errors exist, perform the steps in the following sections to deploy patches, configuration fixes, or both.

Vulnerabilities that require manual fixes or vulnerabilities for which the patch has not been acquired are listed but not available for selection.

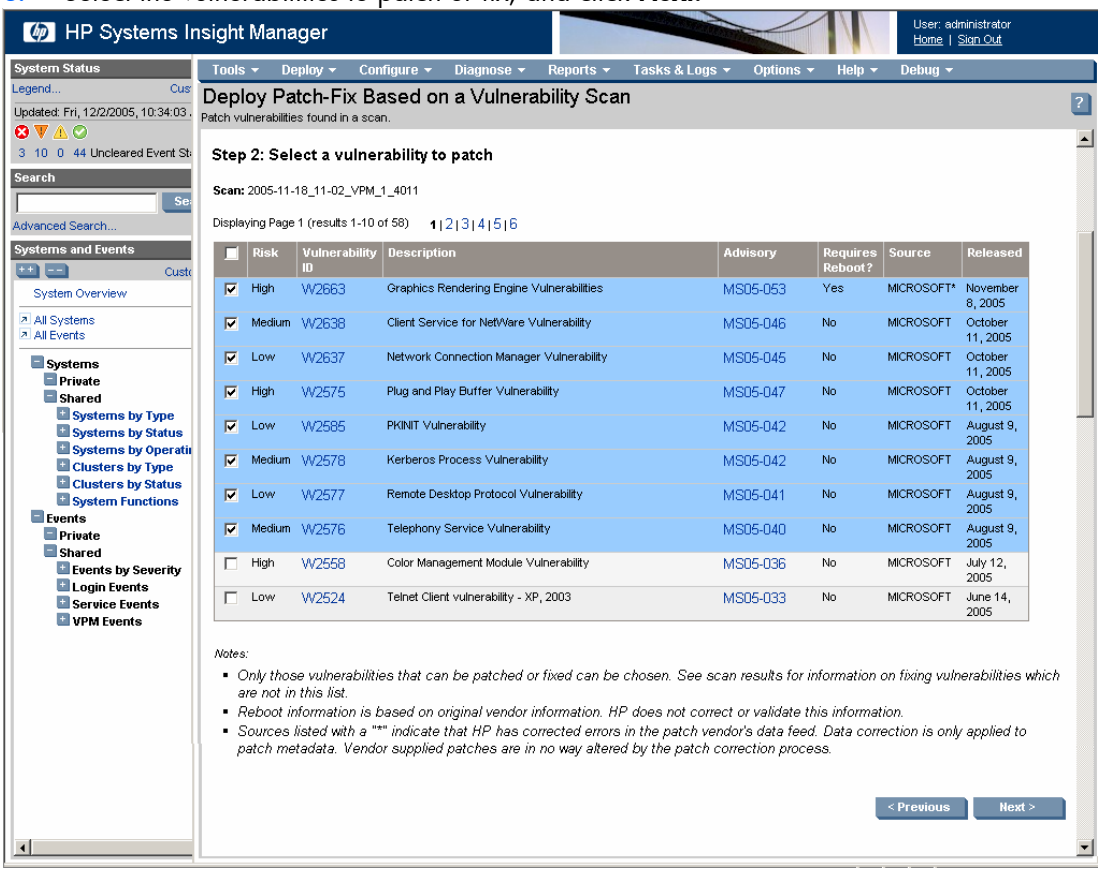
To deploy patches, configuration fixes, or both to systems based on a specific vulnerability scan:

1. Select **Deploy>Vulnerability and Patch Management>Patch-Fix Based on a Scan.**
2. Select the completed vulnerability scan, and click **Next.**

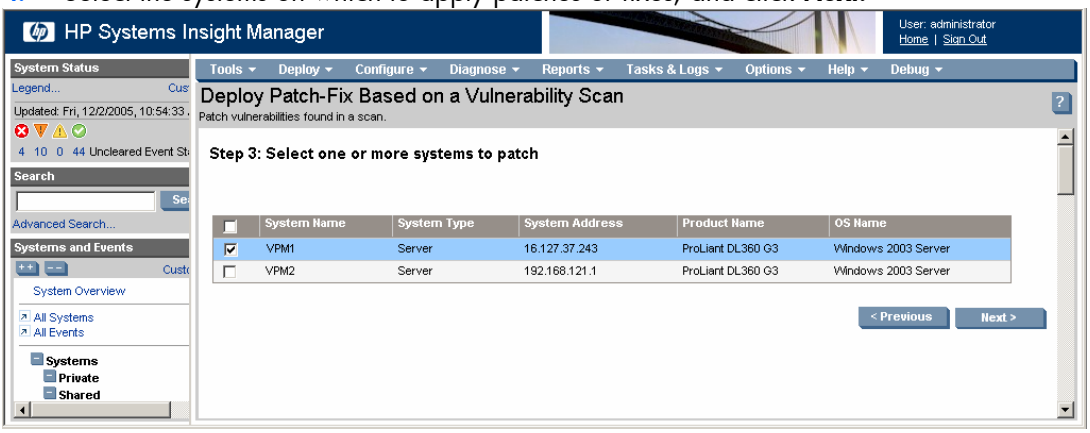


Vulnerabilities appear for all systems included in the scan. All vulnerabilities listed might not be applicable for every system. Clicking the entry in the Vulnerability ID or Advisory column displays additional information about the vulnerability. The Requires Reboot column indicates if the patch requires the system to reboot after deployment.

3. Select the vulnerabilities to patch or fix, and click **Next.**



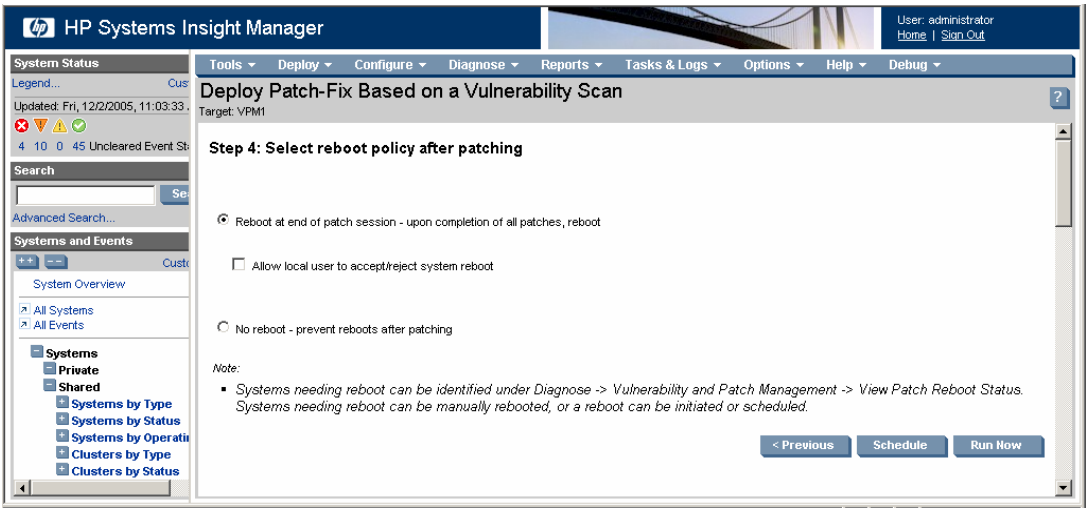
4. Select the systems on which to apply patches or fixes, and click **Next.**



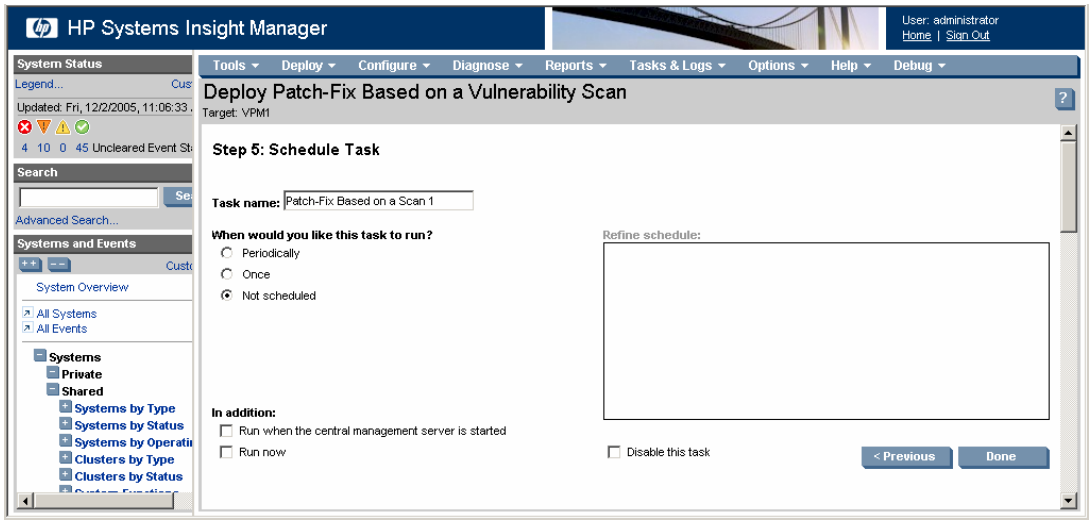
5. Designate when the patched systems will be rebooted. Reboots can be performed immediately after the patches or fixes are installed or postponed until later. The local user can also be given the option to accept or reject the reboot.

NOTE: If the local user rejects the reboot, there will not be another automatic reminder.

6. To deploy patches or fixes immediately, click **Run Now.** To schedule the patch or fix deployment, click **Schedule.**



7. If scheduling the patch or fix deployment:
   c. Enter an appropriate name for the task or accept the default name, and select **Once.**
   d. Designate a time and date to run the task, and click **Done.**



8. View task results in the VPM Events list after the task completes.

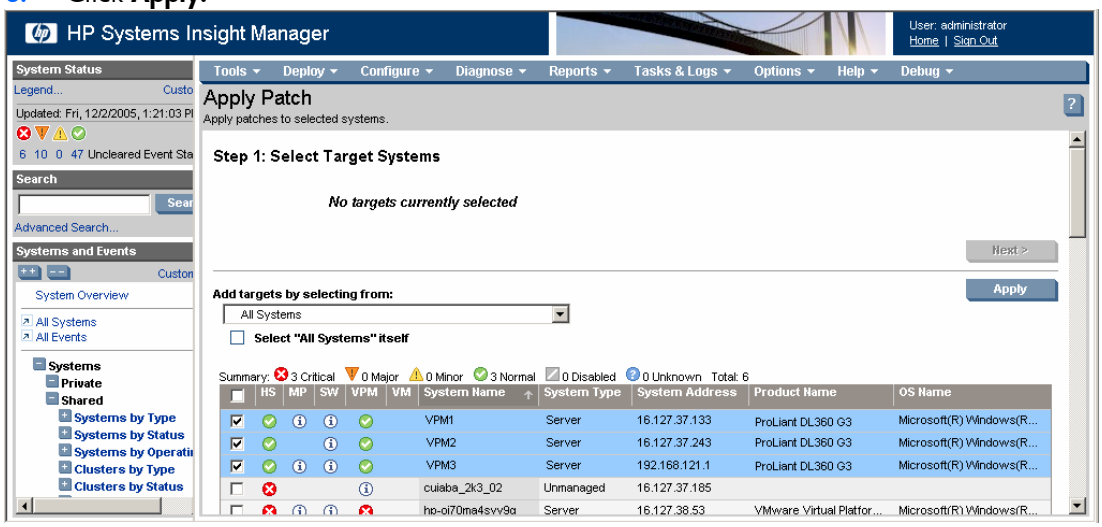
To view the list of target systems that require reboot, see the "Viewing the patch reboot status" section.

Deploying patches without a vulnerability scan

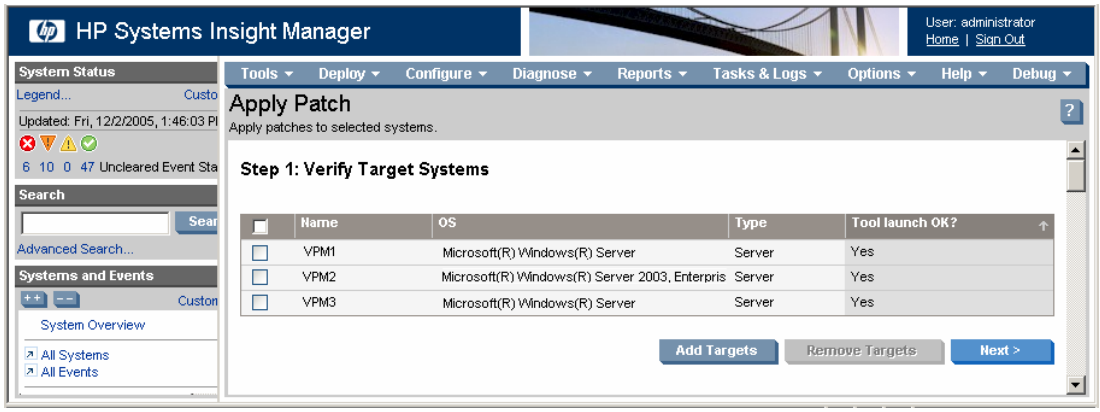
If a patch is released that must be deployed immediately, the patch can be applied without running a scan. In normal circumstances, HP recommends running a scan before deploying patches.

To deploy patches to systems without running a scan:

1. Select **Deploy>Vulnerability and Patch Management>Patch without a Scan.**
2. Select the target systems to patch either by selecting a group from the dropdown list or by selecting the individual systems.
3. Click **Apply.**



4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets,** if necessary to reselect target systems, and click **Next.**



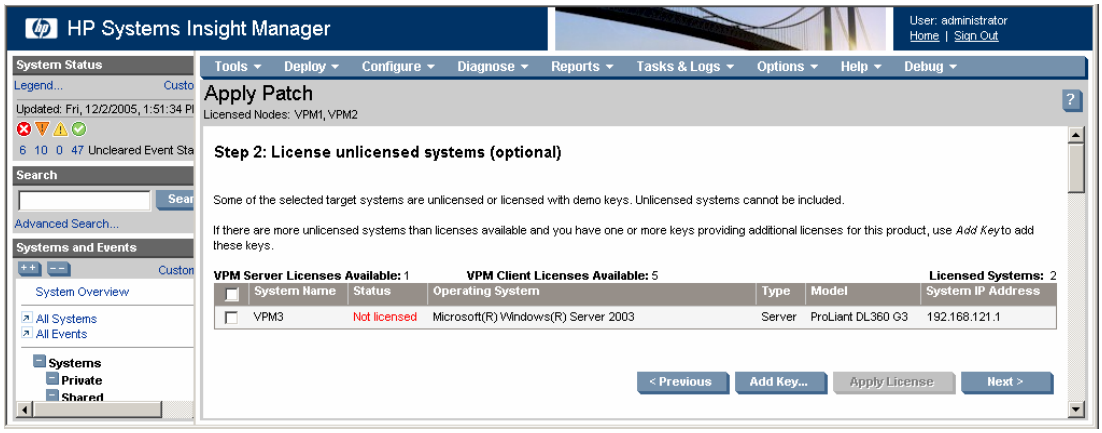
5. If any selected systems are unlicensed or licensed with a time-limited license, permanent licenses can be applied at this time. If licenses are available, select any unlicensed system in the list to license, and click **Apply License.** To add licenses using a key string, click **Add Key**, enter the key string in the field, and click **OK**.

IMPORTANT: If systems listed as Unknown or Unmanaged in HP SIM are selected for licensing, a server license is assumed and automatically applied. HP recommends modifying the HP SIM settings to properly identify systems before licensing.

IMPORTANT: Any unlicensed systems not licensed at this time will not be included in the patch deployment.

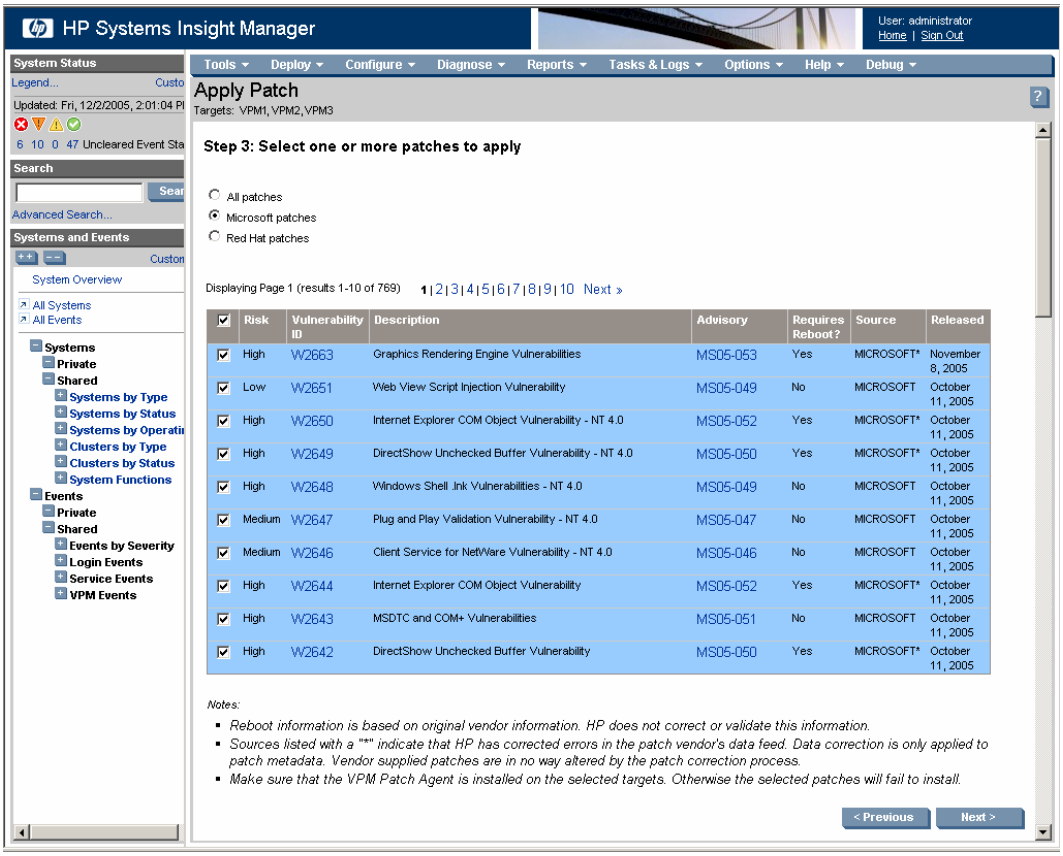
NOTE: If all target systems initially selected for the task are licensed with permanent licenses, the license validation page does not appear.

6. Click **Next**.



All patches included in the patch database appear. Clicking the entry in the Vulnerability ID or Advisory column displays additional information about the patch. The Requires Reboot column indicates if the patch requires the system to reboot after deployment.

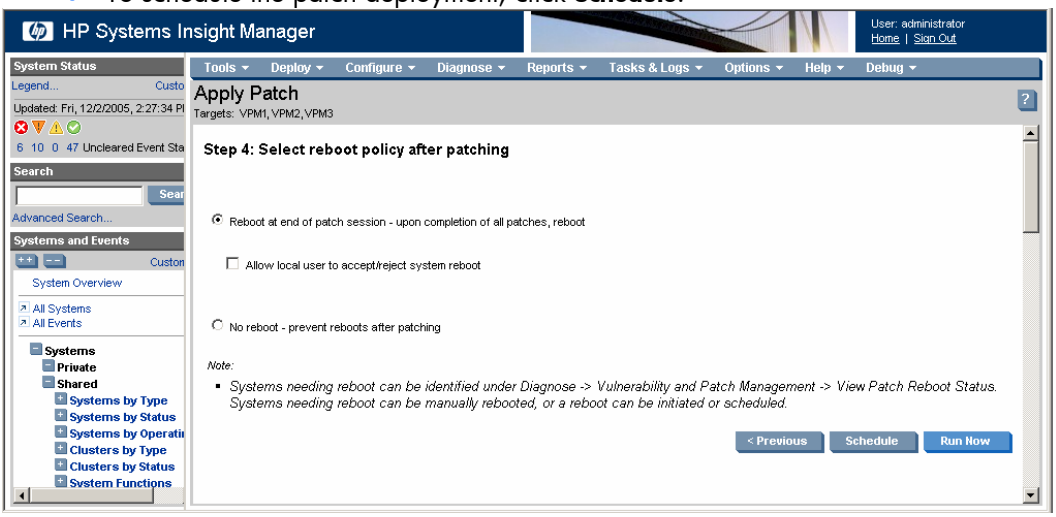
7. Select the vulnerabilities to which to apply patches, and click **Next.**



8. Designate when the patched systems should be rebooted. Reboots can be performed immediately after the patches or fixes are installed or postponed until later. The local user can also be given the option to accept or reject the reboot.

NOTE: If the local user rejects the reboot, there will not be another automatic reminder.

9. To schedule patch deployment, choose one of the following options:
   - To deploy patches immediately, click **Run Now.**
   - To schedule the patch deployment, click **Schedule**.



10. If scheduling the patch deployment:

a. Enter an appropriate name for the deployment task or accept the default name, and select **Once.**

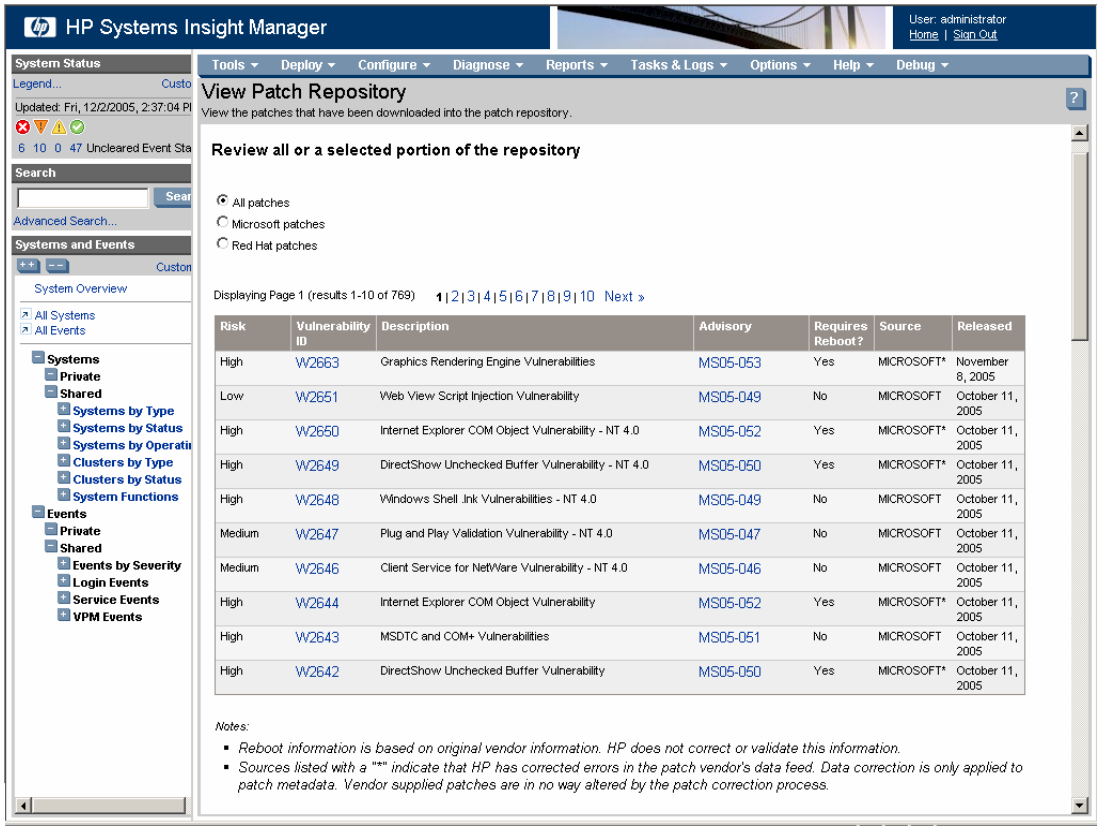
b. Designate a time and date to run the patch deployment task, and click **Done.**

11. View task results in the VPM Events list after the task completes.

To view the list of target systems that require reboot, see the "Viewing the patch reboot status" section.

Viewing the patch repository

1. Select **Diagnose>Vulnerability and Patch Management>View Patch Repository.**
2. To filter the list of displayed patches, select the appropriate patch source from the list. To view information about a specific patch, click the patch identification number in the Advisory or Vulnerability ID column.

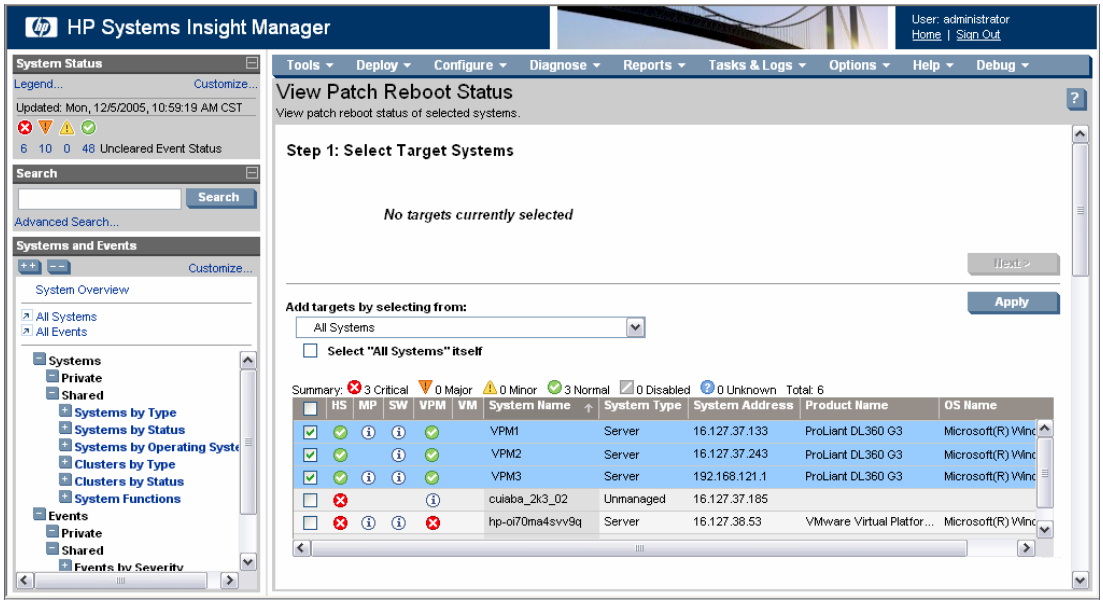


Viewing the patch reboot status

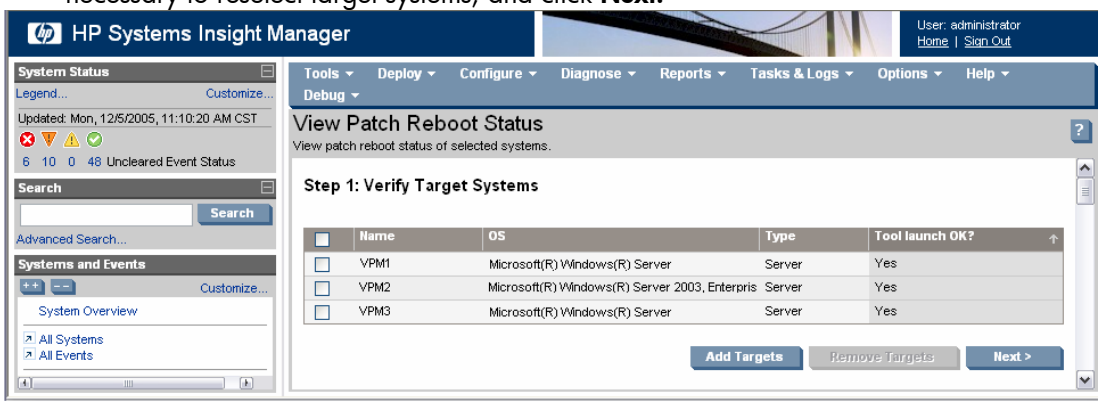
Certain patches require that the server be rebooted after installation. During patch deployment, the option can be selected to reboot the server later. The patch deployment is not complete until after the server has been rebooted.

To view the patch status and initiate reboots for selected systems:

1. Select **Diagnose>Vulnerability and Patch Management>View Patch Reboot Status.**
2. Select the target systems for which to view the reboot status either by selecting a group from the dropdown list or by selecting the checkbox next to individual systems.
3. Click **Apply.**



4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets,** if necessary to reselect target systems, and click **Next.**

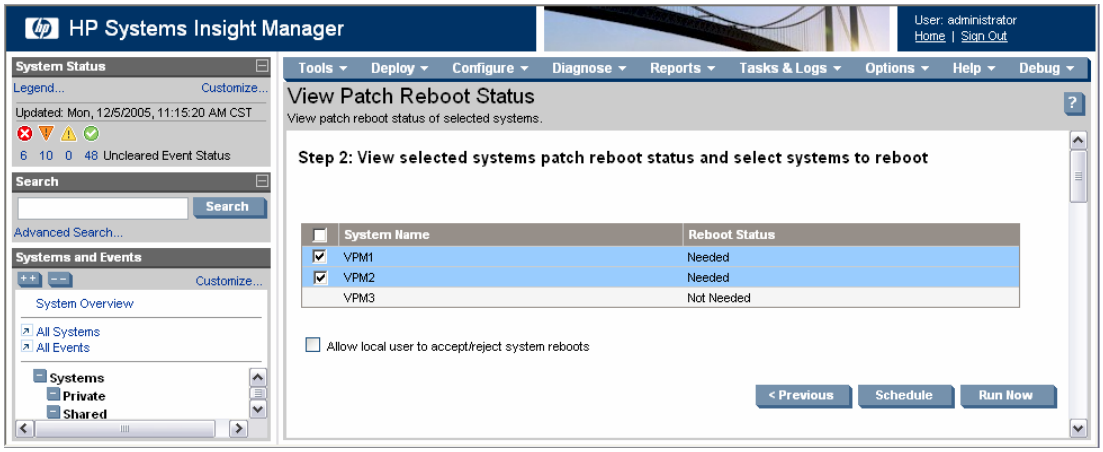


5. The patch reboot status for the selected systems appears in the Reboot Status column. Select the systems to reboot, and select if the local user of all the listed systems will be given the option to accept or reject the reboot.

NOTE: If the local user rejects the reboot, there will not be another automatic reminder.

NOTE: The Reboot Status column does not indicate that reboots are required for systems until after the patch deployment task is complete.

6. To reboot the selected systems immediately, click **Run Now.** To schedule the reboot, click **Schedule.**



7. If scheduling the reboot task:
   a. Enter an appropriate name for the reboot task or accept the default name, and select **Once.**
   b. Designate a time and date to run the reboot task, and click **Done.**

Viewing patch installation status

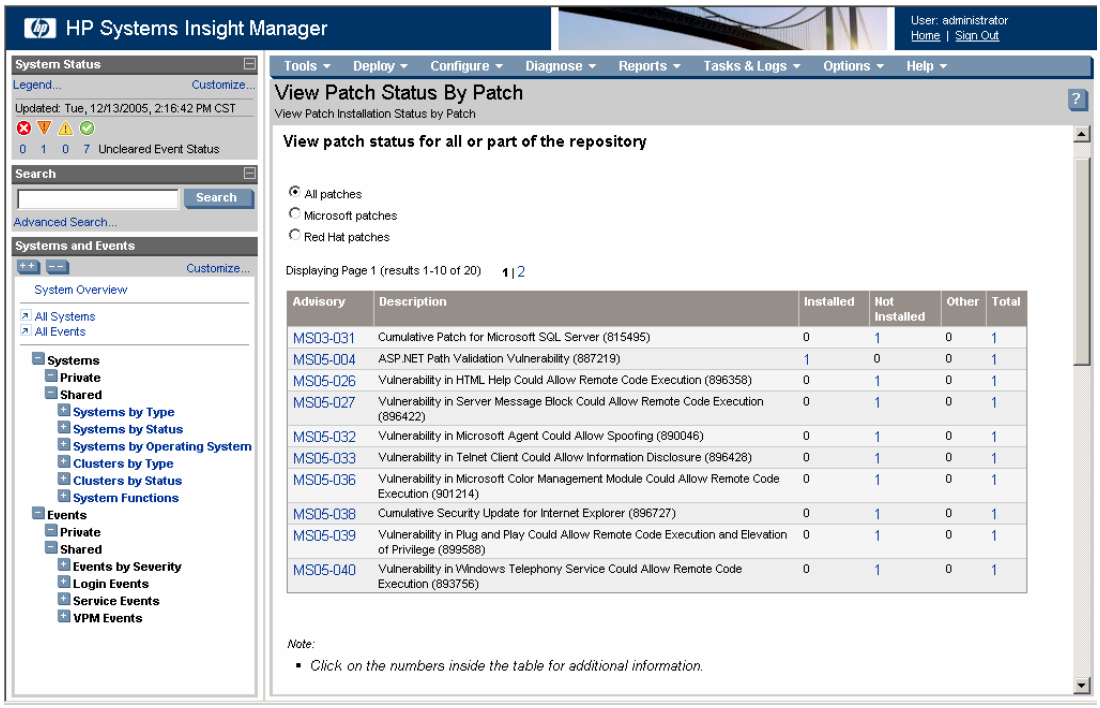
You can view consolidated reports showing patch installation status for all systems managed by Vulnerability and Patch Management Pack. The VPM Patch Agent updates the patch database with a list of all applicable patches, including patches installed by methods other than Vulnerability and Patch Management Pack. Patch reports display the installation status of these patches for each system. The recommended method for determining required patches is performing a vulnerability scan.

You can view reports by systems or patches. A search filter is also available to view the status of a particular patch on a particular system.

Information displayed in patch reports is obtained during the most recent patch deployment or validation task and, therefore, might not be current. The patch installation status can be updated by validating installed patches. For information, see the "Validating installed patches" section.

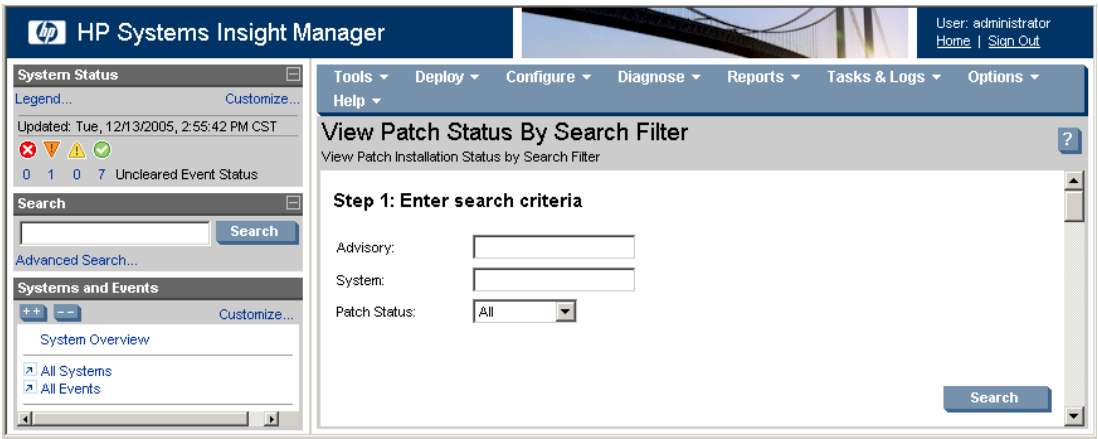
Viewing patch installation status by patch

1. Select **Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View by Patch.**
2. To filter the list of displayed patches, select the appropriate patch source from the list. To view information about a specific patch, click the patch identification number in the Advisory column.

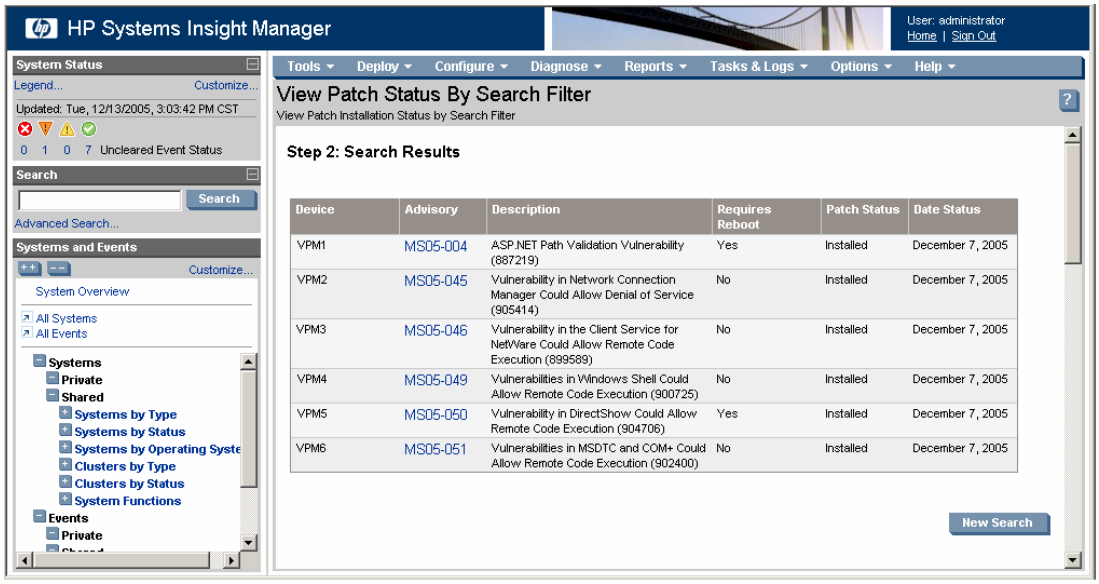


Viewing patch installation status by search filter

1. Select **Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View by Search Filter.**
2. Enter a search parameter in the appropriate field, and click **Search**. You can view patches either by advisory number, target system, or the status of patches. Advisory numbers are in the form MS05-005 or RHSA-2005-05-850.

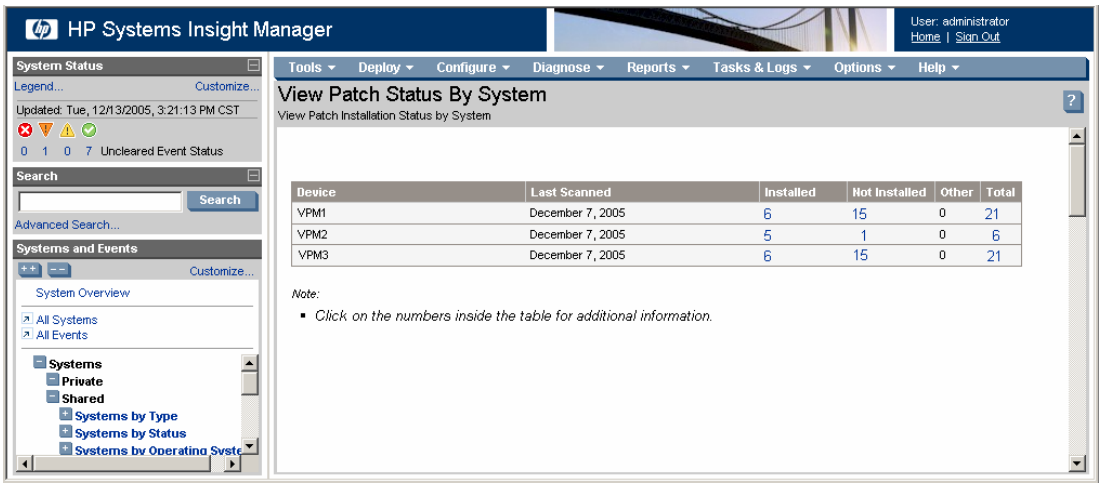


3. To view information about a specific patch, click the patch identification number in the Advisory column.



Viewing patch installation status by system

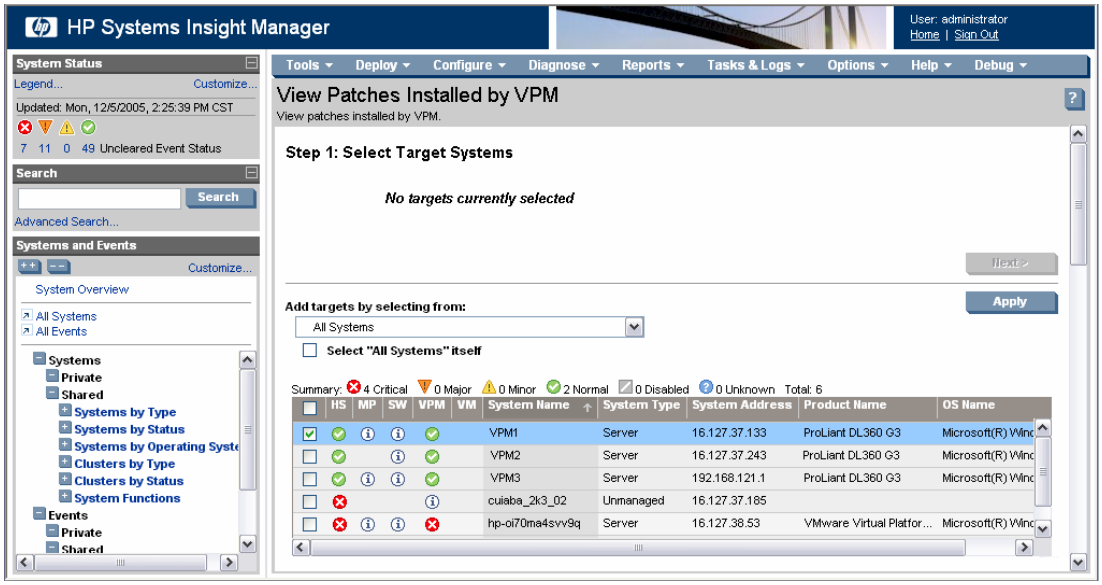
1. Select **Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View by System.**
2. Click the entry in the Installed, Not Installed, or Other column for a system to display additional information about patches for that system. An entry in the Other column indicates that Vulnerability and Patch Management Pack cannot determine if the patch has been installed, possibly because adequate information was not provided by the patch vendor.



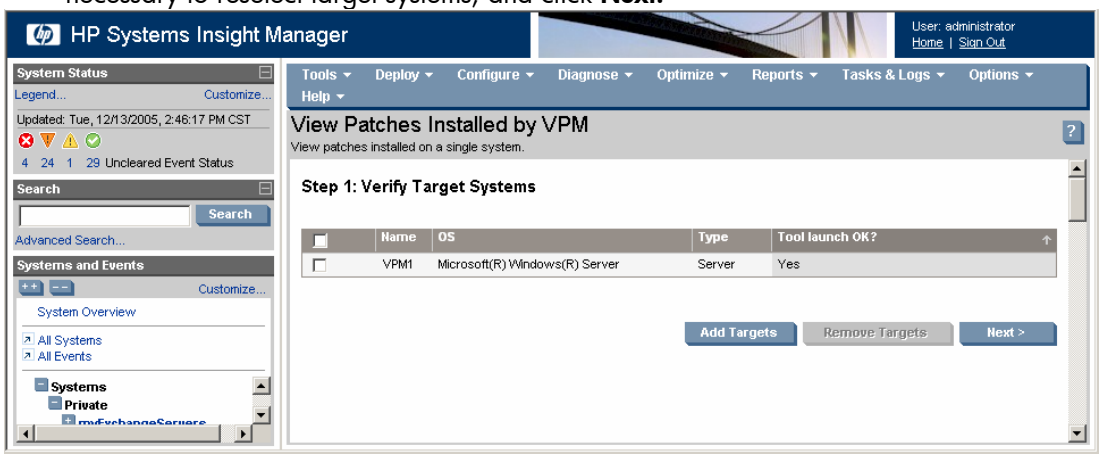
Viewing the patches installed by Vulnerability and Patch Management Pack

A list of patches that have been applied by Vulnerability and Patch Management Pack is maintained for each system. To view the list of patches for an individual system:

1. Select **Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View Patches Installed by VPM.**
2. Select the system for which to view patches installed, and click **Apply.**

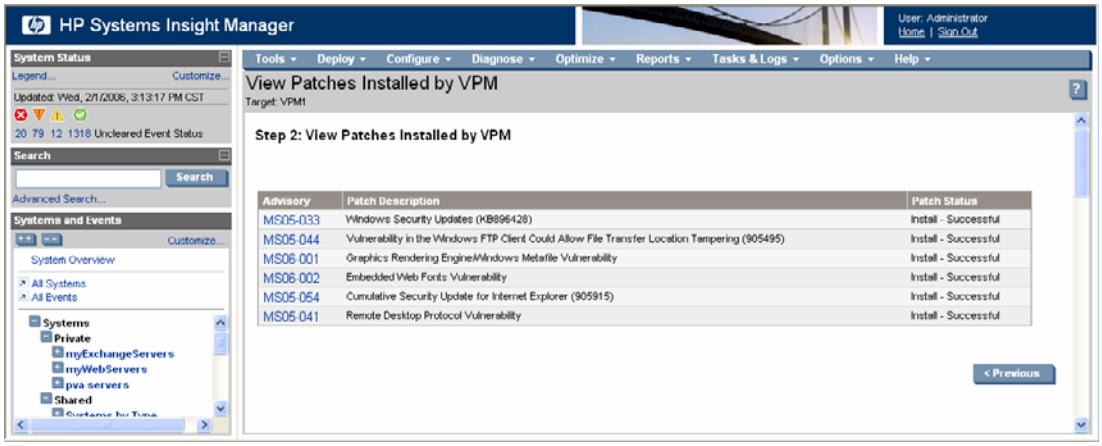


3. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets,** if necessary to reselect target systems, and click **Next.**



The list of patches installed on the system by Vulnerability and Patch Management Pack appears. The Status column indicates one of the following states for each patch:

- Install – Successful—The patch installation completed successfully.
- Install – Unsuccessful—The patch installation did not complete successfully.
- Install – Restore—The patch was previously installed, removed, and restored.
- Reboot Required—The patch requires a reboot, which has not yet been performed.
- Not Applicable—The patch was not installed because it was not needed on this system.

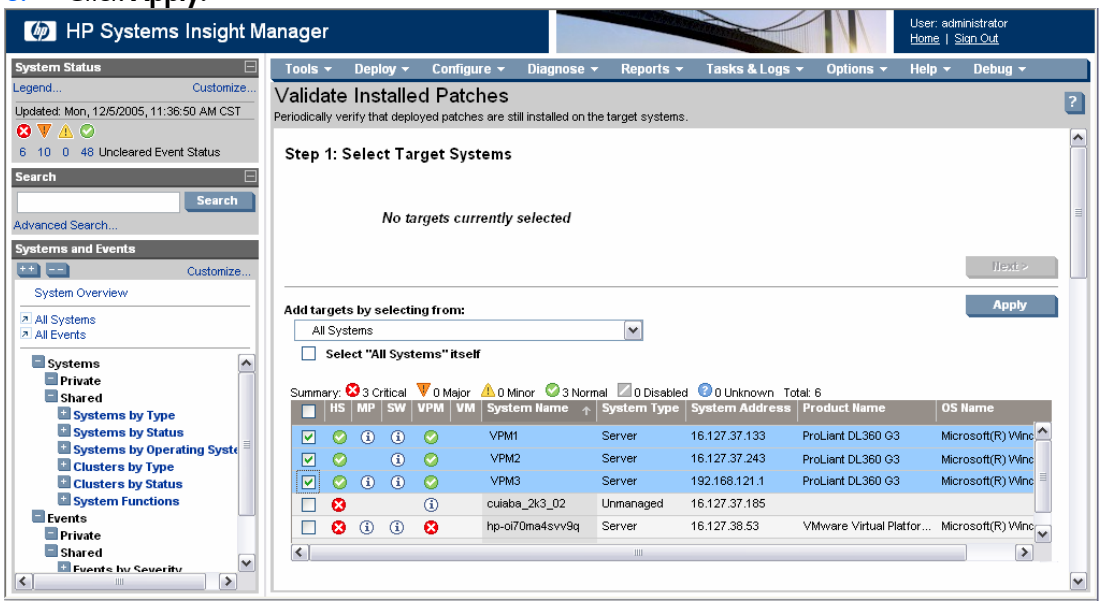


Validating installed patches

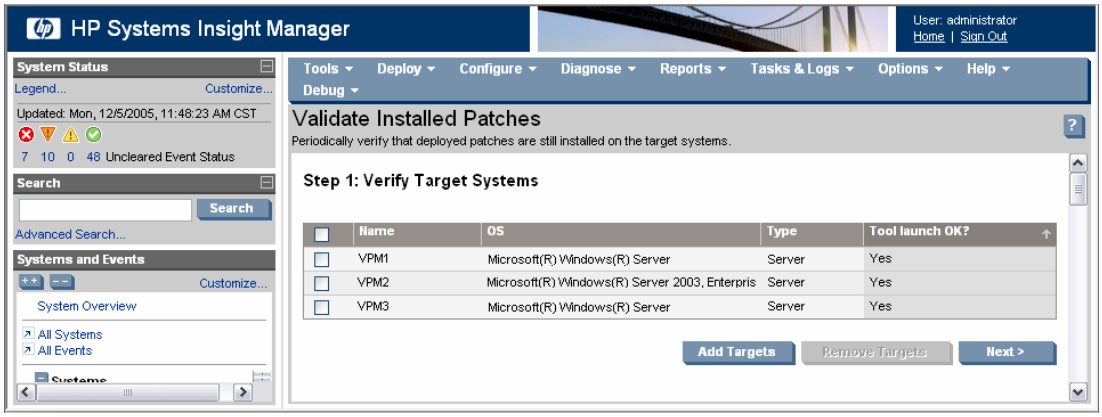
Patch validation identifies any missing patches on target systems and immediately reinstalls the patch, creating a patch deployment event in HP SIM. If a VPM Patch Agent update has been acquired, the update is also automatically applied. If reinstalled patches require selected target systems to be rebooted, this action is automatically deferred. The reboot status can be viewed after a validation task has completed by selecting **Diagnose>Vulnerability and Patch Management>View Patch Reboot Status.**

Schedule a task to periodically verify that deployed patches are still installed on the target systems. Scheduling the task determines how often the VPM Patch Agent performs the verification.

1. Select **Deploy>Vulnerability and Patch Management>Validate Installed Patches.**
2. Select the target systems for which to validate installed patches by selecting a group from the dropdown list or selecting the individual systems.
3. Click **Apply.**

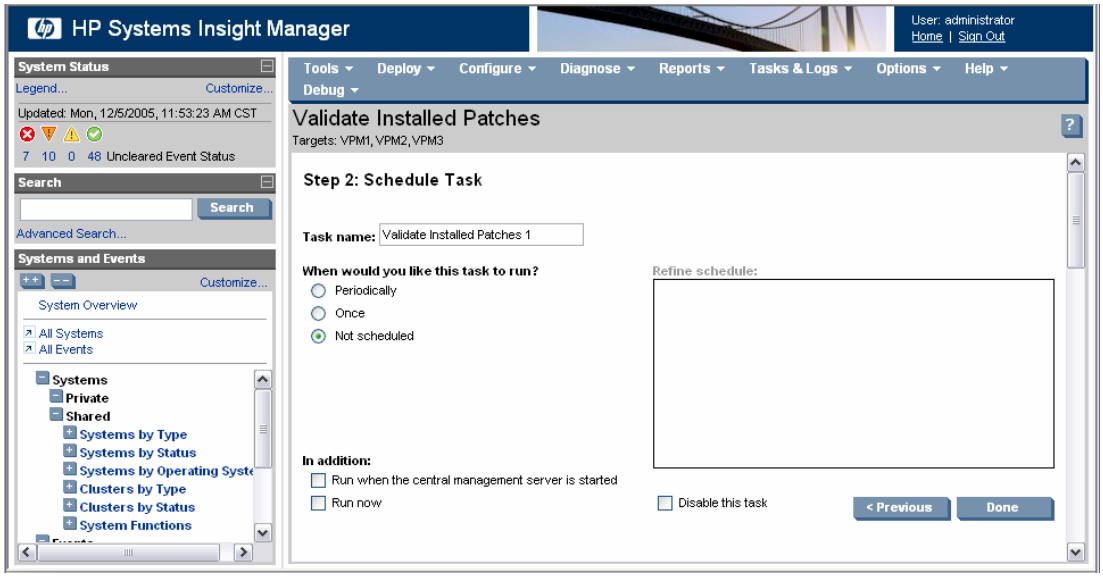


4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets,** if necessary to reselect target systems, and click **Next.**



5. Enter an appropriate name for the validation task, or accept the default name.
6. To schedule the validation task, choose one of the following options:
   - To validate the installed patches immediately, select **Run now,** and click **Done**.
   - To schedule the validation task to run on a regular basis, select **Periodically.**
   - To run the task one time, select **Once**.
7. Designate a time and date to run the validation task, and click **Done.**

NOTE: Multiple patch validation tasks can be scheduled at different frequencies for groups of target systems.



8. View task results in the VPM Events list after the task completes.

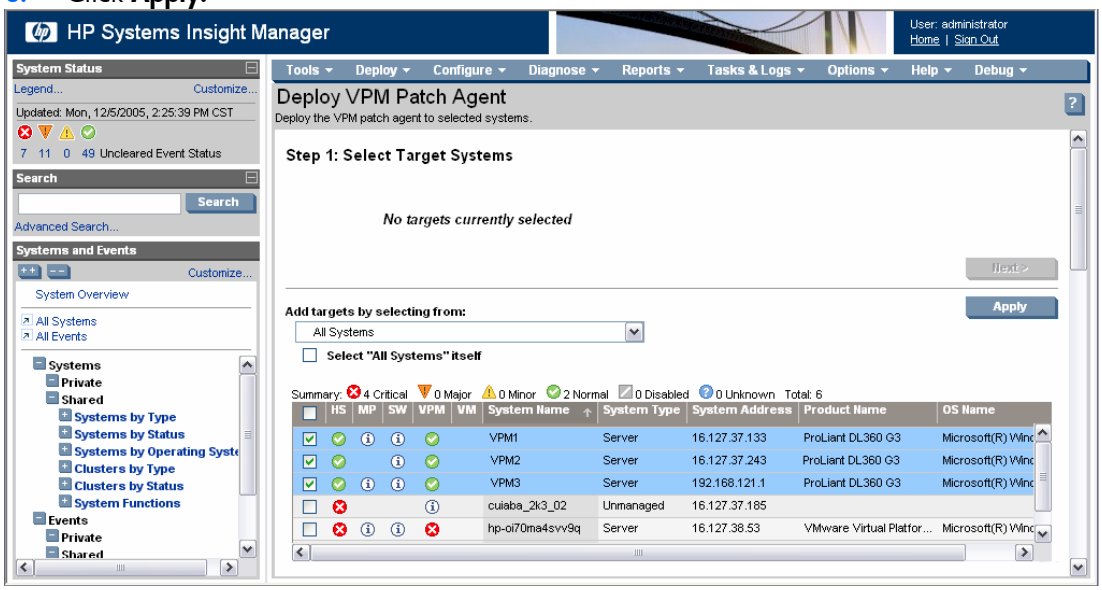
Deploying the VPM Patch Agent

The VPM Patch Agent is automatically deployed when target systems are licensed to allow patches to be applied to the systems. If the VPM Patch Agent is removed from a system for any reason or is not properly deployed to the target system, complete the following instructions to deploy the VPM Patch Agent.

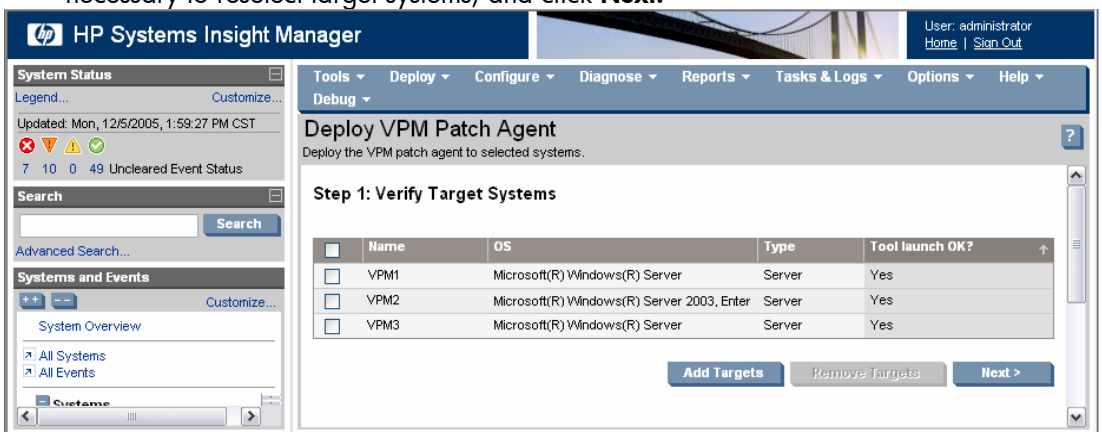
NOTE: If the VPM Patch Agent deployment failed, be sure that the system is accessible by selecting **Options>Protocol Settings>System Protocol Settings** and verifying that the WBEM credentials have been configured properly.

To deploy the VPM Patch Agent to systems to enable patching:

1. Select **Deploy>Vulnerability and Patch Management>VPM Patch Agent.**
2. Select the target systems on which to deploy the VPM Patch Agent either by selecting a group from the dropdown list or by selecting the systems.
3. Click **Apply.**



4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets,** if necessary to reselect target systems, and click **Next.**



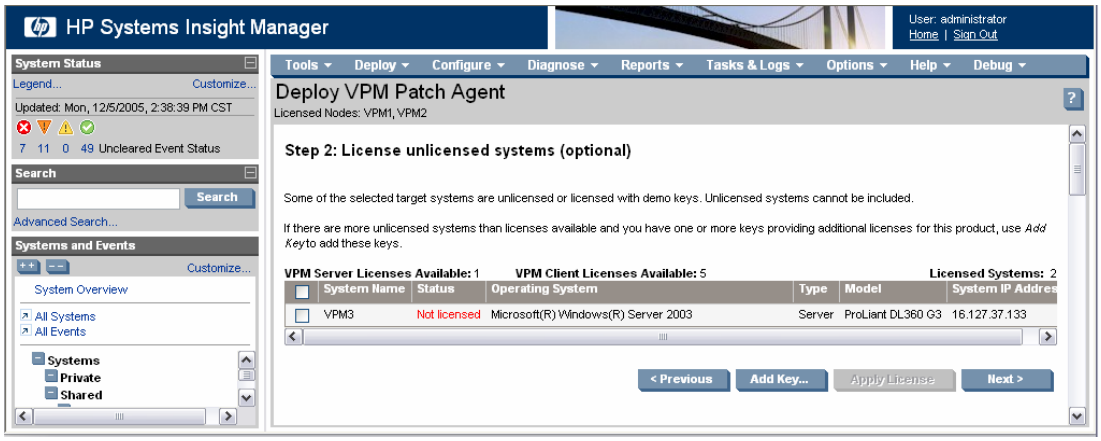
5. If any selected systems are unlicensed or licensed with a time-limited license, permanent licenses can be applied at this time. If licenses are available, select any unlicensed system in the list to license, and click Apply License. To add licenses using a key string, click Add Key, enter the key string in the field, and click **OK**.

IMPORTANT: If systems listed as Unknown or Unmanaged in HP SIM are selected for licensing, a server license is assumed and automatically applied. HP recommends modifying the HP SIM settings to properly identify systems before licensing.

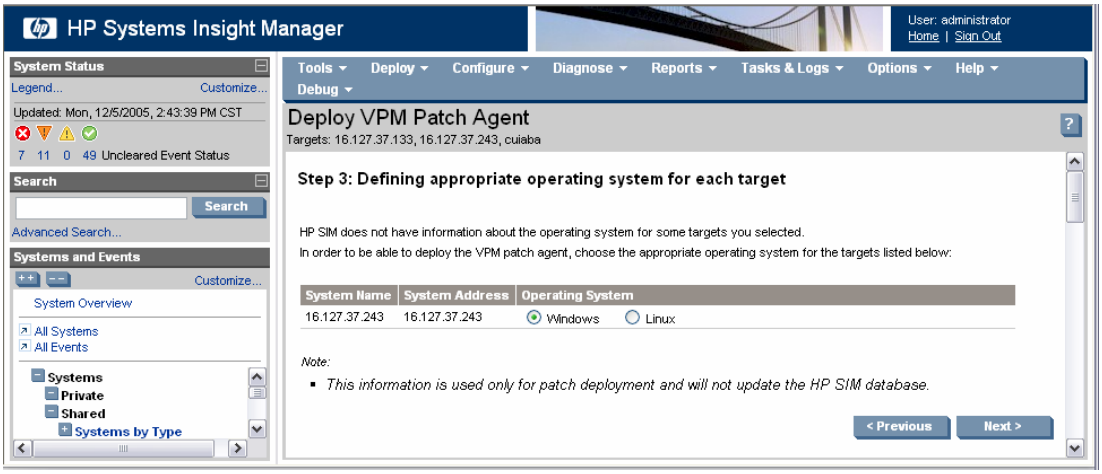
IMPORTANT: Any unlicensed systems not licensed at this time will not be included in the VPM Patch Agent deployment.

NOTE: If all target systems initially selected for the task are licensed with permanent licenses, the license validation page does not appear.

6. Click **Next.**



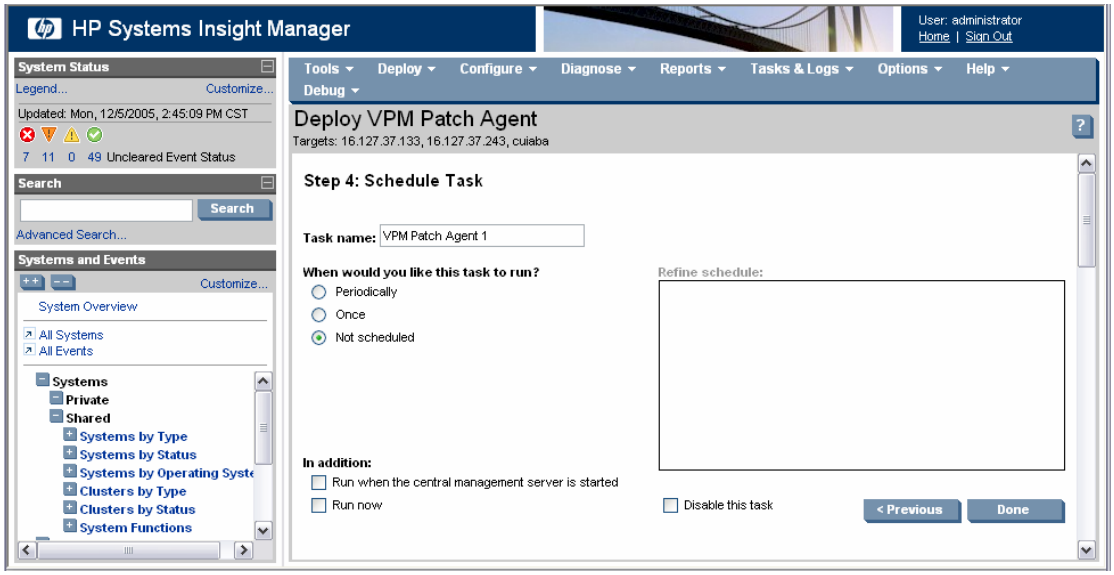
7. If the server type is identified as Unknown or Unmanaged with no identified operating system in the HP SIM console, select the appropriate operating system, and click **Next.**



8. To deploy the VPM Patch Agent immediately, select Run now, and click **Done.**

   To schedule the agent deployment, select **Once,** designate the appropriate date and time, and click **Done.**

NOTE: Patches cannot be applied to systems until after the scheduled task completes and the VPM Patch Agent is applied successfully.



9. View task results in the VPM Events list after the task completes.

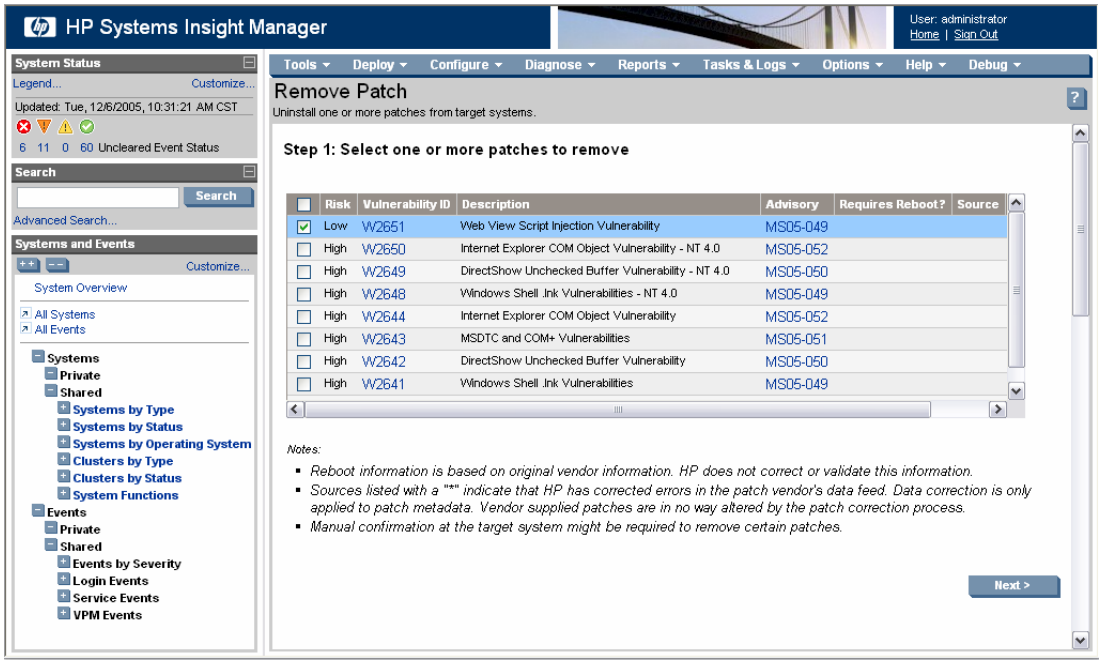
Removing patches

Only patches that can be removed appear on the patch removal page. Only Microsoft patches including vendor-provided uninstallation patches can be removed, provided these patches were installed by Vulnerability and Patch Management Pack. Vulnerability and Patch Management Pack cannot remove configuration fixes or Red Hat patches. Vulnerability and Patch Management Pack does not perform dependency checking before removing patches. HP recommends extreme care when removing patches.

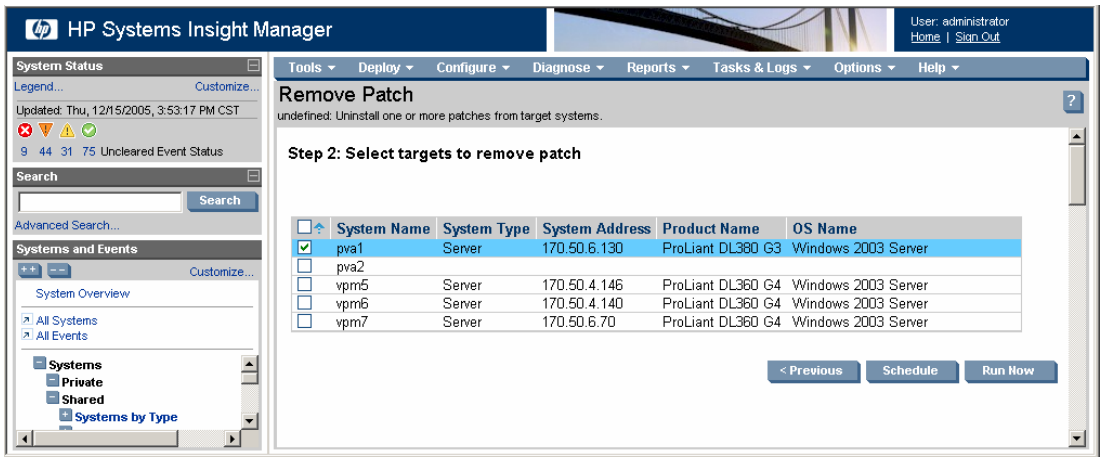
To remove patches after they have been applied to systems:

1. Select **Deploy>Vulnerability and Patch Management>Remove Patch.**
2. Select the patches to remove, and click **Next.**

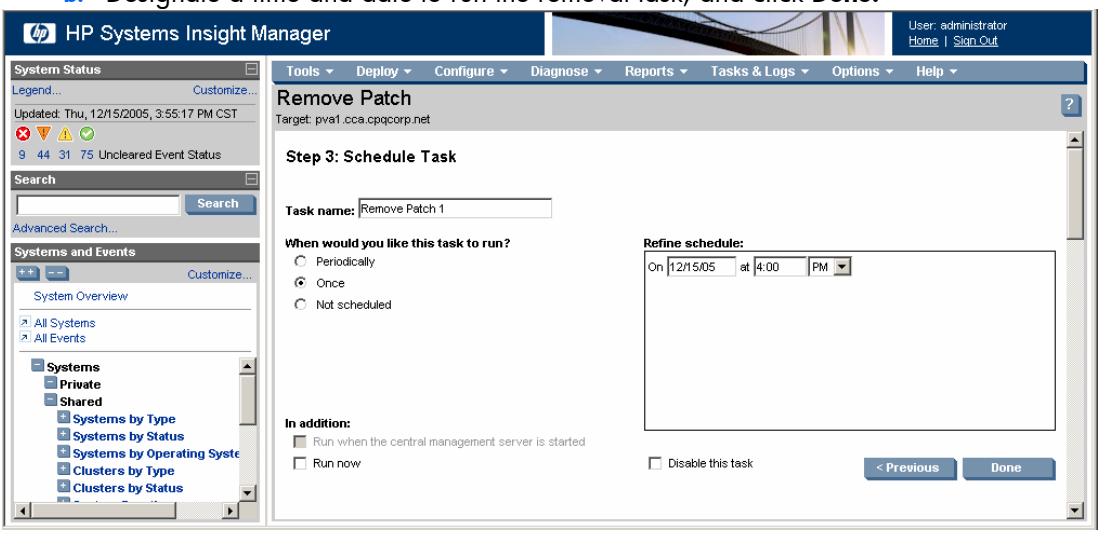
NOTE: Manual reboot of the target system might be required to remove certain patches.



3. Select the systems on which to remove the designated patches.
4. To remove the patches immediately, click **Run Now.** To schedule the patch removal, click **Schedule.**



5. If scheduling the patch removal task:
   a. Enter an appropriate name for the removal task or accept the default name, and select **Once.**
   b. Designate a time and date to run the removal task, and click **Done.**



6. View task results in the VPM Events list after the task completes.

If the patch removal requires the target system to be rebooted, this action is automatically deferred. The reboot status can be viewed after a patch removal task has completed by selecting **Diagnose>Vulnerability and Patch Management>View Patch Reboot Status.**

Troubleshooting

This section identifies and provides solutions for commonly encountered issues, as well as answers to frequently asked questions. The following topics are included:

- Vulnerability and Patch Management Pack installation and configuration
- Vulnerability scans
- Patches and configuration fixes
- HP SIM integration

Vulnerability and Patch Management Pack installation and configuration

Viewing Vulnerability and Patch Management Pack installation logs

The Vulnerability and Patch Management Pack installation logs, which list the details of the installation of each Vulnerability and Patch Management Pack component, are located at %HOMEDRIVE%:\vpmsetuplogs, where HOMEDRIVE is usually the C drive. You can view the following logs:

- vmpsetup.log—Contains log information from the main installer, including calls and result codes from the execution of component installers
- vmpsrvsetup.log—Contains log information about the creation of the Vulnerability and Patch Management Pack directories and menus in the VPM server
- vmpsimsetup.log—Contains log information from the HP SIM component installation
- RCS.log—Contains information about the installation of the Radia Configuration Server, which manages vulnerabilities based on policies established by HP SIM
- RPS.log—Contains information about the installation of the Radia Proxy Server, which is used as the central patch repository
- RMS.log—Contains information about the installation of the Radia Messaging Server, which is a messaging service used to communicate Vulnerability and Patch Management Pack status information
- RPM.log—Contains information about the installation of the Radia Patch Manager (Server), which acquires security patches from the Internet, loads them into the Radia Configuration Server, and synchronizes this information in the database
- RMP.log—Contains information about the installation of the Radia Management Portal, which is used to initiate the installation of the VPM Patch Agent and perform Vulnerability and Patch Management Pack actions on remote systems
- Radiawrp.log—Contains an installation summary of the previous five components

Vulnerability and Patch Management Pack installation updates MDAC and MSDE

If MSDE or files used by MSDE are not up-to-date, files are updated during the Vulnerability and Patch Management Pack installation. The server is rebooted after updated files are installed. In this situation, the Vulnerability and Patch Management Pack installation must be restarted.

An error occurs when installing MSDE files from a Remote Desktop session

Install Vulnerability and Patch Management Pack using the system console instead of a Remote Desktop session. For additional information, see **http://support.microsoft.com/default.aspx?scid=kb;en-us;246694&sd=tech**.

Vulnerability and Patch Management Pack installation fails with `There Are No Configuration Files` error

This error occurs because the metabase, the configuration files used for IIS, has been corrupted. To resolve:

1. Download metaedit from **http://download.microsoft.com/download/iis50/utility/5.0/NT45/EN-US/MtaEdt22.exe**.
2. Double-click **MtaEdt22.exe.**
3. Locate **STATScanner** at LM\W3SVC\1\ROOT, and click **Delete.**
4. Restart the Vulnerability and Patch Management Pack installation.

`STAT Scanner WSI Requires IWAM and IUSR` error occurs during Vulnerability and Patch Management Pack installation

This occurs when the server name has been changed after IIS was installed. IIS must be uninstalled and reinstalled before Vulnerability and Patch Management Pack can be installed.

Installation fails with `Product RMS not installed: Service RMS error. The specified service does not exist as an installed service (0x424)`

If the password of the account used to install Vulnerability and Patch Management Pack contains curly braces, "{" or "}," the Radia component installation fails. To correct this, either complete the following steps to temporarily change the install account password or create a new local account with administrator privileges to use to perform the installation.

1. Change the password to remove the illegal characters.
2. Select **Start>Control Panel>Administrative Tools>Services.**
3. Right-click **HP Systems Insight Manager,** and select **Properties.**

4. Click the **Log On** tab, and update with the new password.
5. Click the **General** tab, and click **Stop>Start** to restart the HP SIM service.
6. Right-click **IIS Admin Service,** and select **Restart.** Click **Yes** to confirm.

Proceed with the Vulnerability and Patch Management Pack installation. If necessary, the installation account credentials can be changed back after the installation completes. Repeat steps 2 through 6 after the password has been changed, and then see the "Using the Change VPM Credentials Utility" section to update the Vulnerability and Pack Management Pack password.

Vulnerability and Patch Management Pack installation fails

- Be sure the VPM server can effectively communicate with other networking components, such as the database and HP SIM server (if separate).
- If the VPM server has multiple IP addresses, be sure Name Resolution is used for both
- If IPv6 is enabled, uninstall from the network interface card being utilized for Vulnerability and Patch Management Pack communication.
- If the Vulnerability and Patch Management Pack installation was attempted multiple times, reboot before attempting the installation again.

Cannot modify VPM acquisition settings to acquire updates from a local repository

A patch acquisition must have already been run using the VPM Acquisition Utility and saved to the designated directory before VPM acquisition settings can be modified to acquire updates from a local repository. For information about acquiring patches using the VPM Acquisition Utility, see the "Acquisitions using the VPM Acquisition Utility" section.

Required open ports

The following ports must be open on target systems to allow successful scanning with Vulnerability and Patch Management Pack:

IMPORTANT: If a proxy server is used, it must be configured to allow both HTTP and FTP traffic.

NOTE: These ports are opened automatically when Vulnerability and Patch Management Pack is installed on a Windows XP SP2 system. By default, Internet Connection Firewall closes some of these ports. Be sure that the ports listed are open.

- TCP 22—SSH
- TCP 135, 137, 138, 139, 443, and 445—NetBIOS and SSL, used by the Vulnerability and Patch Management Pack scanning components
- TCP 2301 and 49400—HP Management Agents
- TCP 3463, 3464, 3466, and 3465—Used by Vulnerability and Patch Management Pack patching components

The following ports must be open on the VPM server:

- TCP 80—HTTP Web server, if an HTTP connection is used between the VPM and HP SIM servers (TCP 443 must be open if an HTTPS connection is used)
- TCP 445—MSDE named pipes communications

- UDP 1433, 1434—MSDE Shared Instance Support
- TCP (variable)—MSDE TCP/IP communications. This port, assigned at random by MSDE during installation, can be identified by selecting **Start>Run,** entering svrnetcn.exe, and clicking **OK.** Select **Computername\Device** from the Server Instances dropdown menu. In the Enabled Protocols list, select **TCP/IP>Properties.** The port number appears. The port number can be changed at this time, if necessary.

The following ports are used by HP SIM and must be open:

- TCP 22—SSH
- UDP 161—SNMP
- UDP 162—SNMP trap
- TCP 280—HTTP
- TCP 5989—WBEM/WMI Mapper secure
- TCP 50000—HTTPS
- TCP 50001—Secure SOAP
- TCP and UDP 53—DNS

Modifying firewall configuration settings

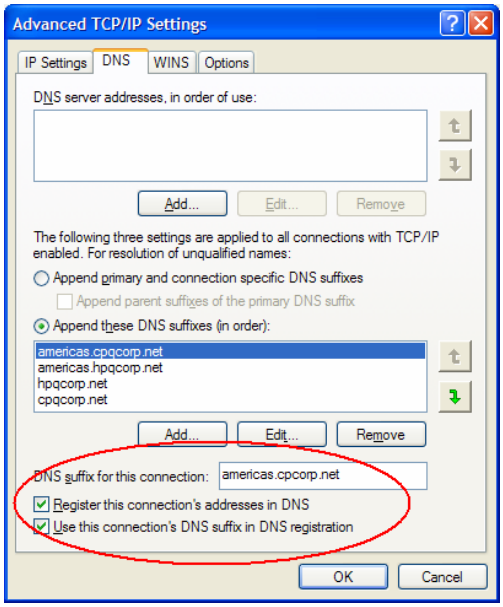
To ensure that Vulnerability and Patch Management Pack can obtain updates, be sure that your firewall is configured for access to **ftp://ftp.hp.com/pub/essentials/vpm/**.

Configuring a DNS server

If no DNS server exists in the server network, update the host files on both the HP SIM and VPM servers (if separate) with the IP and Network Naming. These files are located at C:\Windows\system32\Drivers\etc. The target systems must be able to resolve the VPM server name to an IP address.

The server host name where HP SIM and VPM are installed must be correctly configured for name resolution and reverse lookup. To determine if DNS is properly configured, use the `nslookup` command, passing both the host IP address and the fully qualified hostname.

If using DHCP, verify the following configurations in the advanced TCP/IP properties:



Be sure that the DNS suffix for this connection field has the correct DNS suffix and that both the **Register this connection's addressees in DNS** and **Use this connection's DNS suffix in DNS registration** are selected.

All target systems do not have the same administrator credentials

For target systems that have individual administrator credentials, configure WBEM credentials individually to enable access to these target systems.

1. From within HP SIM, select **Options>Protocol Settings>System Protocol Settings.**
2. Select the system to configure, and click **Apply.**
3. Enter the appropriate WBEM credentials, and click **Run Now.**

Multiple VPM servers

Target systems cannot be scanned and patched by multiple VPM servers. The deployed VPM Patch Agent is set up to respond to only one VPM server.

Administrator credentials have been changed

If the administrator credentials have been changed for target systems, the WBEM credentials must be reconfigured. To reconfigure Global Protocol Setting, select **Options>Protocol Settings>Global Protocol Settings.** To reconfigure System Protocol Settings, select **Options>Protocol Settings>System Protocol Settings.**

Changing the IIS IWAM user name and password

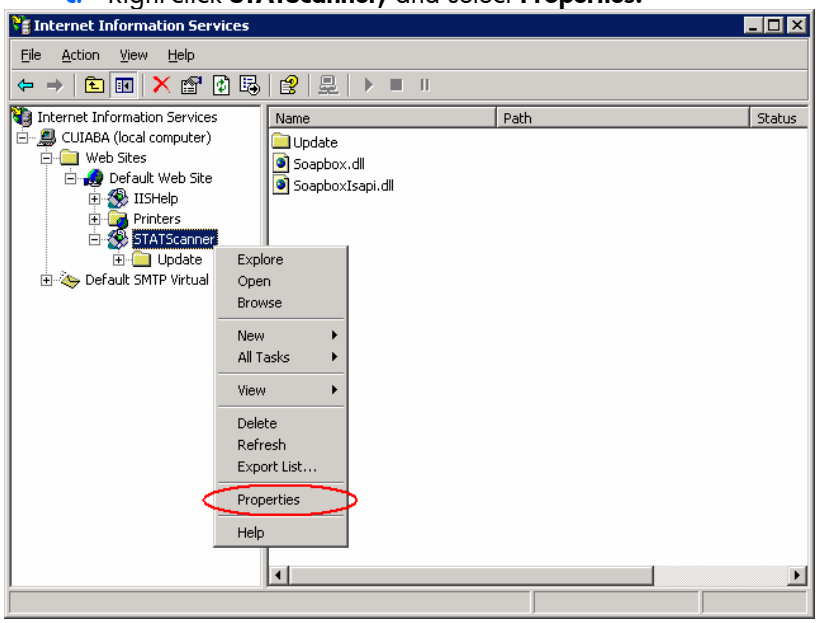
HP recommends that the IWAM_*hostname* and IUSR_*hostname* accounts not be modified after they are installed by IIS. Modifying these accounts corrupts the rights and security privileges of Vulnerability and Patch Management Pack and IIS components.

For information about backing up and restoring the ISS Metabase, see http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/131b609d-ff3a-488f-a8dd-13044fa623a1.mspx

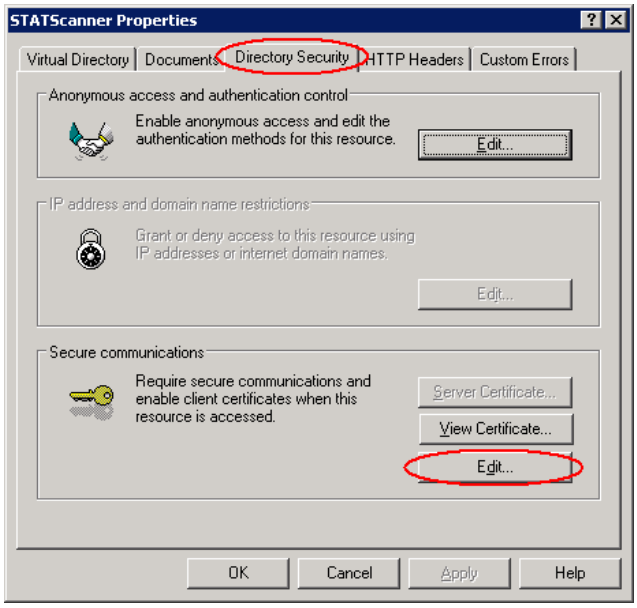
The IIS Certificate has expired and the Vulnerability and Patch Management Pack connection must be reconfigured to use an HTTP connection

HP recommends using a secure HTTPS connection between the HP SIM server and the VPM server, when these components are installed on separate servers. However, if you currently have an HTTPS connection that must be reconfigured to HTTP:

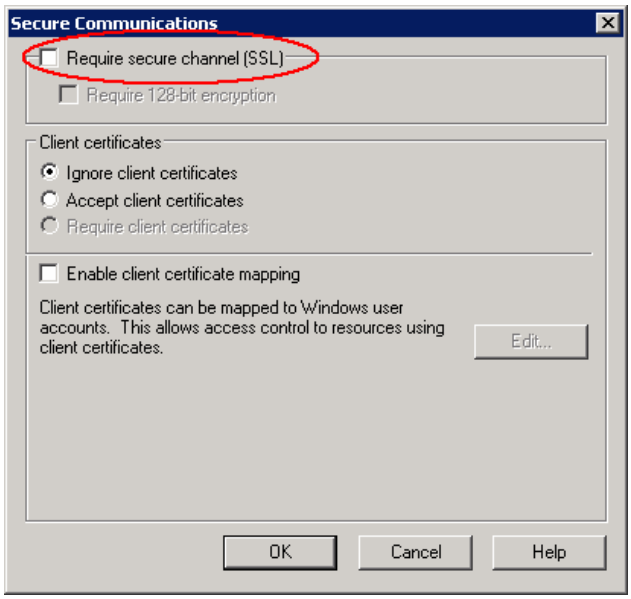
1. Remove the SSL certificate from IIS.
2. Change the IIS configuration to accept both HTTP and HTTPS connections:
   a. Open Internet Information Services Manager.
   b. Locate **STATScanner** under Default Web Site on the local computer.
   c. Right-click **STATScanner,** and select **Properties.**



   d. Click the **Directory Security** tab.
   e. Click **Edit** in the Secure Communications field.



f. Clear the Require secure channel (SSL) option, and click **OK**>**OK**.



Uninstalling Vulnerability and Patch Management Pack

Use either of the following methods to uninstall Vulnerability and Patch Management Pack. The Vulnerability and Patch Management Pack uninstallation must be performed from the VPM server.

Vulnerability and Patch Management Pack scan results can be retained after uninstallation. The last scan performed can be accessed from the VPM column. If you choose to delete scan results, the VPM column is set to an initialized state. See the "Hiding the VPM column in the HP SIM console" section to hide the VPM column.

IMPORTANT: Be sure that no vulnerability scans, patch deployments, or patch acquisitions are running. Close all browsers before attempting to uninstall Vulnerability and Patch Management Pack.

IMPORTANT: Vulnerability and Patch Management Pack licenses are not removed from target systems when Vulnerability and Patch Management Pack is uninstalled.

To uninstall with the Vulnerability and Patch Management Pack uninstaller:

1. Select **Start>Programs>HP ProLiant Essentials Vulnerability and Patch Management>Uninstall Vulnerability and Patch Management.**
2. When prompted, select whether to remove the Vulnerability and Patch Management Pack data stored on the HP SIM server, such as scan reports and Vulnerability and Patch Management Pack tasks. Data displayed in the HP SIM systems list is cleared if data is removed.
3. When prompted, select whether to remove the patch database.
4. When uninstall is complete, the HP SIM service is automatically restarted.
5. Delete the VPM directory. Its default location is: C:\Program Files\HP\VPM.

To uninstall from the Control Panel:

1. Select **Add or Remove Programs.**
2. Select **HP Vulnerability and Patch Management>Change/Remove.**
3. When prompted, select whether to remove the Vulnerability and Patch Management Pack data stored on the HP SIM server, such as scan reports and Vulnerability and Patch Management Pack tasks. Data displayed in the HP SIM systems list is cleared if data is removed.
4. When prompted, select whether to remove the patch database.
5. When uninstall is complete, the HP SIM service is automatically restarted.
6. Delete the VPM directory. Its default installation location is: C:\Program Files\HP\VPM.

Remaining Vulnerability and Patch Management Pack files

A Vulnerability and Patch Management Pack uninstallation does not remove all Vulnerability and Patch Management Pack files from the server. The following files remain after uninstallation:

- C:\Novadigm\ManagementAgent\nvdkit.exe
- C:\Novadigm\ ManagementAgent\rma.tkd
- C:\Novadigm\ ManagementAgent\ rma.log
- C:\Program Files\HP\Systems Insight Mnager\hpwebadmin\webapps\ROOT\mxportal\VPM\column\vpmcolmain.jps
- C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\VPM\column\vpmbase.html
- C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\home\STATScanner

NOTE: The VPM Results directory only remains if you select to retain Vulnerability and Patch Management Pack data during the uninstallation.

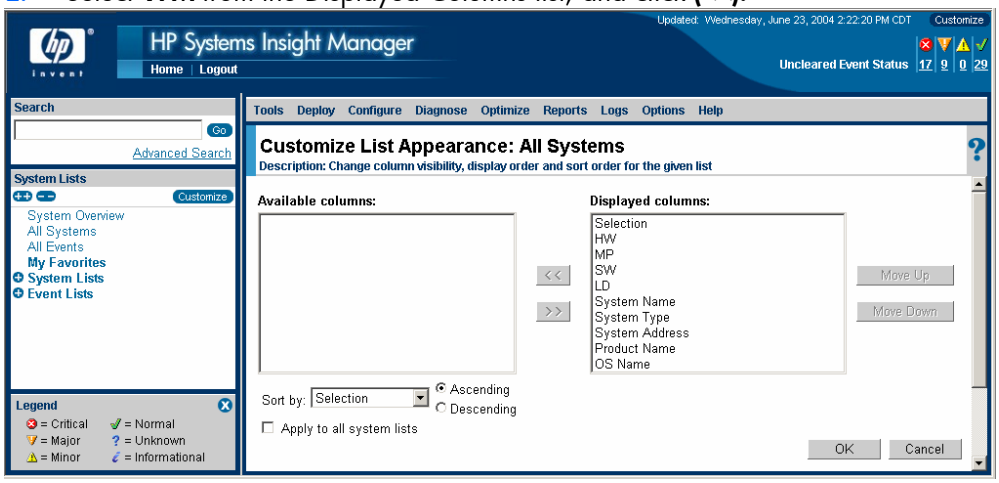
- C:\Program Files\Microsoft SQL Server\MSSQL$VPMMSSQL\Data\ radiadb.mdf
- C:\Program Files\Microsoft SQL Server\MSSQL$VPMMSSQL\Data\ radialog.ldf

NOTE: These files only remain if you select to retain the patch database during uninstallation.

Hiding the VPM column in the HP SIM console

Vulnerability and Patch Management Pack uses the VPM column in the HP SIM console to identify vulnerability status. If Vulnerability and Patch Management Pack has been uninstalled, vulnerability status information is no longer updated in the HP SIM console. Data displayed in the HP SIM systems list is cleared if Vulnerability and Patch Management Pack data is removed during uninstallation. To hide the column in the HP SIM console after Vulnerability and Patch Management Pack has been uninstalled:

1. Click **Customize** in the top right corner of the All Systems frame.
2. Select **VPM** from the Displayed Columns list, and click **(<<).**



3. Click **OK.**

Reinstalling Vulnerability and Patch Management Pack

If an updated version of Vulnerability and Patch Management Pack is installed after a previous version has been uninstalled, the entitlement list could be lost for all managed target systems. To prevent this, be sure that you uninstall and reinstall the updated VPM Patch Agent to all target systems.

Radia uses installation account instead of local account

To accommodate a security modification contained in Windows 2003 SP1, the Vulnerability and Patch Management Pack installer modifies the Windows service running httpd (Radia Integration Server) to use the installation account rather than the Local System account. In addition, the installation account is modified to run as a service.

Vulnerability scans

Vulnerability and Patch Management Pack cannot access target systems

If Vulnerability and Patch Management Pack cannot perform accurate scanning on a target system because of access problems, verify the following information depending on the target operating system.

Windows

- The account used to scan the target system is a member of the Administrator group or Domain Administrator group for that system.
- Client for Microsoft Networks is installed and enabled.
- Vulnerability and Patch Management Pack has share-level access to all target systems.
- Remote Registry Service is started.
- File and Printer Sharing protocol is installed and enabled.
- Default Administrative Shares are enabled.
- Server Service is started.
- Simple File Sharing is disabled.
- The Internet Connection Firewall is configured correctly or disabled, and the target system is configured to respond to ping commands.
- The Computer Name/Domain network component is defined.

Windows XP

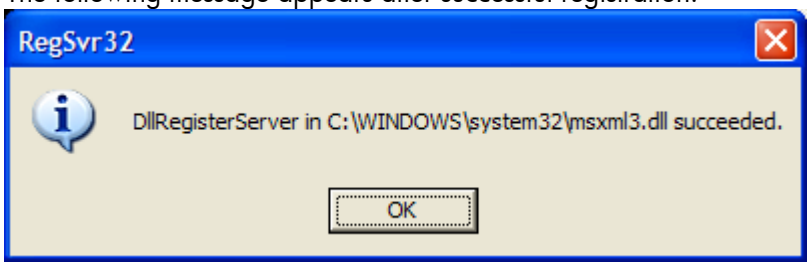
Verify that Simple File Sharing is disabled on Windows XP Professional machines that are not part of a domain. Simple File Sharing is enabled by default, disabling network access to Administrative shares on the machine.

Windows VPM server

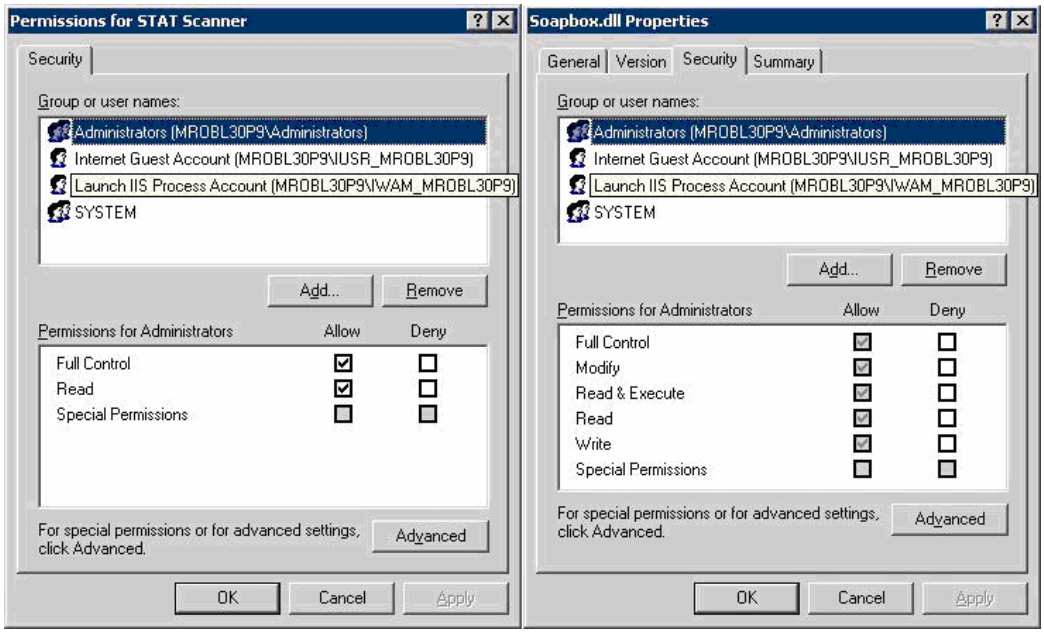
STAT scanner cannot connect to HP SIM if the file, msxml3.dll, is not registered on the Windows XP system.

1. Execute the following command at the command prompt to verify the existence of the file:
   `dir %SystemRoot%\system32\msxml3.dll`
2. If the file is not registered, execute the following command at the command prompt to force the registration: `regsvr32 %SystemRoot%\system32\msxml3.dll`

The following message appears after successful registration:



Also, ensure that the IWAM_*xxx* account has adequate privileges to function properly. Appropriate file permissions and Microsoft Windows NT® registry permissions must exist for the resources to function properly. See the following figure for examples.



Configure file permissions on all necessary DLLs. Configure Windows NT Registry permissions on the following:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\STAT Scanner
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\STAT Scanner WSI

Linux target systems

- TCP/IP network protocol is enabled.
- SSH is enabled and listening on the default port 22.
- Vulnerability and Patch Management Pack includes PuTTY SSH client and uses the plink session command and PSCP secure copy, as well as SFTP secure file transfer commands. Both protocols 1.5 and 2.0 are supported if they are correctly installed and functioning on the target system. To determine which protocol is running, telnet to port 22 on the target system, read the return banner, and press the **Enter** key.
  - SSH-1.5—Only protocol 1.5 is supported.
  - SSH-1.9—Protocol 1.5 and 2.0 are supported. Protocol 1.5 is attempted first.
  - SSH-2.0—Only protocol 2.0 is supported, the newest and preferred session protocol.

Scan reports cannot be viewed

If scan reports cannot be viewed in .pdf format because Adobe Acrobat cannot be launched, perform the following procedure:

1. From Internet Explorer, select **Tools>Internet Options.**
2. Click the **Advanced** tab, and scroll to **Security.**
3. Clear the **Do not save encrypted pages to disk** option, and click **OK.**

For more information, see **http://support.microsoft.com/default.aspx?scid=kb;en-us;812935&Product=ie600**.

A scan was submitted but never started

All target systems scanned by Vulnerability and Patch Management Pack must have an IP address displayed in the HP SIM console. If a scan is requested for a target system with no IP address, the scan does not run and an internal error is generated. Be sure that all target systems being scanned have IP addresses that appear in the HP SIM console.

Scan results are inaccurate because of overlapping tasks

When scheduling vulnerability scans and patches, be sure the two processes do not overlap. Allow adequate time for a vulnerability scan to complete before starting a patch. If a patch deployment runs during a vulnerability scan, the scan results might be inaccurate or the target systems might reboot during the scan.

Do not schedule patch acquisition tasks to run while vulnerability scans are running. Patch acquisition tasks cause vulnerability scans to abort.

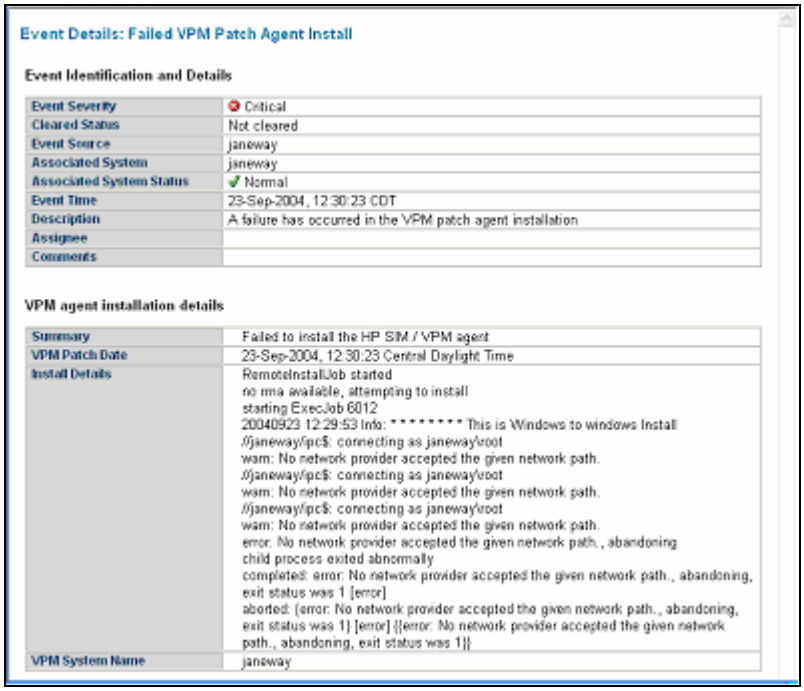
Current patch information is not displayed in scan reports

Scan definition updates are available a few days after the release of patches. You might have a patch in your patch repository that does not appear in your scan results. You can apply the patch without a scan. The VPM Patch Agent will not apply patches that are not appropriate. With the new patch reports, you can also use the Validate VPM Patch Agent operation to determine where patches are needed. This operation applies to patches only. The VPM Patch Agent does not report on non-patch security vulnerabilities.

Patches and configuration fixes

VPM Patch Agent install fails

The VPM Patch Agent is automatically deployed when systems are licensed to allow patches to be applied to the systems. If a server type is identified as Unknown or Unmanaged with no identified operating system in the HP SIM console, Vulnerability and Patch Management Pack automatically attempts to deploy the VPM Patch Agent for Windows systems. The VPM Patch Agent deployment fails on Linux systems, and event details display an error.



To deploy the VPM Patch Agent to target systems, see the "Deploying the VPM Patch Agent" section. Be sure that the Red Hat library, compat-libstdc++, is installed on Red Hat target systems.

The VPM Patch Agent installation can also fail because the WBEM credentials are not configured properly to allow Vulnerability and Patch Management Pack to access target systems. For information about configuring WBEM credentials, see the "Post-installation configuration" section.

A patch acquisition was started, but no patches are seen

A patch acquisition can take quite a bit of time the first time it is run. It is not unusual for the acquisition to take more than four hours, depending on how many operating systems are selected for download and the speed of the Internet connection.

Progress of the acquisition can be monitored at C:\Program Files\HP\VPM\Radia\IntegrationServer\logs\patch-acquire.log. If the log file indicates that no patches are being acquired and there is a proxy server in the environment, be sure you have properly configured Vulnerability and Patch Management Pack to access the proxy server by selecting **Options>Vulnerability and Patch Management>Settings.** In addition, the proxy server must be configured to allow both HTTP and FTP traffic.

If the patch-acquire.log is not being updated, the acquisition process might be hung. Search the patch-acquire.log for the start of the last logged process id. Stop the nvdkit.exe with that process id running on your VPM server. This action terminates the current acquisition and allows the next acquisition to run.

HTTP 300 errors received during patch acquisition

Patch acquisition can generate events containing HTTP 300 errors for some older Microsoft patches, such as:

```
Error downloading patch data for Bulletin MS02-050 at URL
http://www.microsoft.com/ntserver/terminalserver/downloads/
critical/q329115/default.asp error code 300
```

This message occurs because the Microsoft information pertaining to the patch location is incorrect and the patch cannot be downloaded. HP is working to correct the metadata at the HP/Radia website for these older patches, however this is ongoing maintenance. These corrections will automatically be downloaded each time a patch acquisition is run. No updates are needed to Vulnerability and Patch Management Pack.

Patches appear in a scan report but are not successfully deployed

This can occur in the following situations:

- A vulnerability scan has identified vulnerabilities, patches were selected for deployment based on the scan, and one or more of the selected patches were not located in the patch repository. Generally, some of the patches will install successfully, while others do not install for an extended time. Patches might not be available in the patch repository because all of the necessary operating systems were not selected for patch acquisition or only some of the patches have been acquired.
- The VPM Patch Agent has not been successfully installed on the system being patched.
- A patch deployment is attempted on a system for which the patch is not applicable. Vulnerability and Patch Management Pack applies patches to target systems based on the operating system characteristics and patch vulnerabilities. For example, a patch cannot be deployed when a Red Hat patch is selected for deployment on a Windows target system.

Check for missing patches

Be sure that a patch acquisition has been selected for all operating systems in the server environment. Different Microsoft patches can exist for each operating system associated with an advisory. To validate if a patch has been acquired, click the advisory link to the operating system vendor. The patches for each operating system are listed. Check the C:\Program Files\HP\VPM\Radia\IntegrationServer\Data\Patch\Microsoft\<*bulletin number*> directory to see if each patch has been acquired.

Check the file C:\Program Files\HP\VPM\Radia\IntegrationServer\Logs\patch-acquire.log for a history of the last patch acquisition, including any errors. Patches downloaded through HTTP might have been acquired successfully, but those requiring FTP are failing. If this occurs, validate the proxy and firewall settings to be sure they are configured properly to enable FTP traffic.

Validating VPM Patch Agent installation

Check the VPM events to see if a successful Installed VPM Patch Agent event exists for the system to be patched. If no event is present or if a Failed VPM Patch Agent Install event exists, select **Deploy>Vulnerability and Patch Manager>VPM Patch Agent** to deploy the agent.

After the VPM Patch Agent installation and patch acquisition have been verified, reinitiate the patch installation by selecting **Deploy>Vulnerability and Patch Manager>Validate Installed Patches.**

Patch installation status reports are not current or do not match information displayed in scan reports

Information displayed in patch reports is obtained during the most recent patch deployment task. If this information is not current, update the patch installation status by validating installed patches. For information, see the "Validating installed patches" section.

Other tools report that a Windows system is patched, but Vulnerability and Patch Management Pack reports patches needed

Many other tools read the registry to determine if a patch is installed. In many cases, when a patch installation fails, the registry is updated while the files remain unchanged. Vulnerability and Patch Management Pack verifies that both the files and registry keys have been updated.

Patch source for vendor patches is Microsoft* or Red Hat*

To determine patch applicability, Vulnerability and Patch Management Pack might enhance patch detection criteria to be more precise than vendor information. These patches appear with an asterisk in the Patch Source column. HP does not modify the patch itself.

Multiple events listed in HP SIM for patch deployments

Patch deployments create multiple events in HP SIM. There is a start event, a completion event, and a patch current status event. The patch current status event evaluates the status of the patches after the reboot has been completed.

STAT Scanner update error listed in the HP SIM event log

If STAT Scanner cannot access certain necessary files during a patch acquisition scanner update, a 3010 error appears in the HP SIM event log. The file update will be completed the next time a reboot is performed.

Radia internal error listed in the HP SIM event log

A generic Radia internal error appears in the HP SIM event log if the patch repository is viewed before a patch acquisition had been performed.

`Abuse of Service` error occurs when attempting to acquire Red Hat patches

The Red Hat network might be disabled if the network determines that patches have been acquired too frequently. To resolve this issue, delete the registered system from the Red Hat network Web interface at **https://rhn.redhat.com**. Recreate the Red Hat credentials on the Red Hat server and copy to the VPM server.

Validate Installed Patches event does not complete

Certain Vulnerability and Patch Management Pack events cannot complete successfully until after a system has been scanned and patched at least one time. Be sure a system has been scanned and patched before attempting to validate installed patches.

HP SIM integration

Vulnerability and Patch Management Pack menus do not appear in the HP SIM console after installation

The tool menus might not appear after a Vulnerability and Patch Management Pack installation for any of the following reasons:

- The HP SIM user does not have appropriate privileges to access the menus. If a new HP SIM user cannot view the Vulnerability and Patch Management Pack menus, be sure that the user is authorized for All Tools or VPM Tools in Options>Security>Users and Authentication.
- A successful installation of Vulnerability and Patch Management Pack requires the user to have CMS administrative privileges because changes are made to the HP SIM core and the tool menus.
- When installing Vulnerability and Patch Management Pack, you must use the credentials previously used when installing HP SIM. Failure to do so results in an incorrect installation. Also, the user name will not have appropriate privileges. Be sure the CMS user has privileges (toolbox, authorizations) to use Vulnerability and Patch Management Pack. If the authorization is not correct, the menus do not appear. To correct this issue, uninstall Vulnerability and Patch Management Pack and reinstall using the correct credentials. Be sure that the CMS user that will be using Vulnerability and Patch Management Pack has appropriate privileges. This can include having authorization for a toolbox containing the Vulnerability and Patch Management Pack tools.
- The Vulnerability and Patch Management Pack installation failed. Installation errors appear on-screen during installation and in the log files.

Vulnerability and Patch Management Pack provided scan definitions

The following table lists the provided scan definitions that are provided with Vulnerability and Patch Management Pack and a brief description of each.

NOTE: Custom scans can be created from the default system scans. When default system scans are updated, the custom scans are updated with corresponding vulnerability updates also.

Table 5 Provided scan definitions

Scan definition	Description
4_0*	Windows NT® 4.0 vulnerabilities
Advisory	Microsoft Advisories
AutoFix	Autofixable vulnerabilities
CrossPlatform	Windows and Linux vulnerabilities
FileChecks	Known and unknown locations file checks
FileCheck_KnownLocation	Known location file checks
FileCheck_UnknownLocation	Unknown location file checks
IE	Internet Explorer vulnerabilities
IIS	IIS vulnerabilities
Linux	Linux vulnerabilities
Malware	Malware checks
Password	Password policy check
PasswordChecker	Windows NT password policy
Policy	All policy check
SqlServer	SQL Server vulnerabilities
W2K	Windows 2000 vulnerabilities
W2K3	Windows 2003 vulnerabilities
XP	Windows XP vulnerabilities

* This scan definition is not included with the current version of Vulnerability and Patch Management Pack and will only exist if previous versions of the software have been installed.

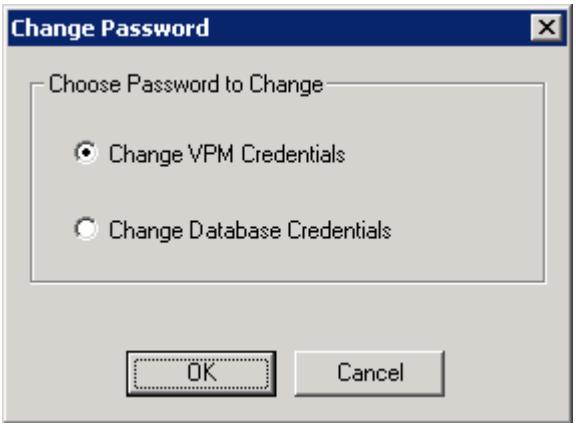
Using the Change VPM Credentials Utility

The Change VPM Credentials Utility can be used to update Vulnerability and Patch Management Pack:

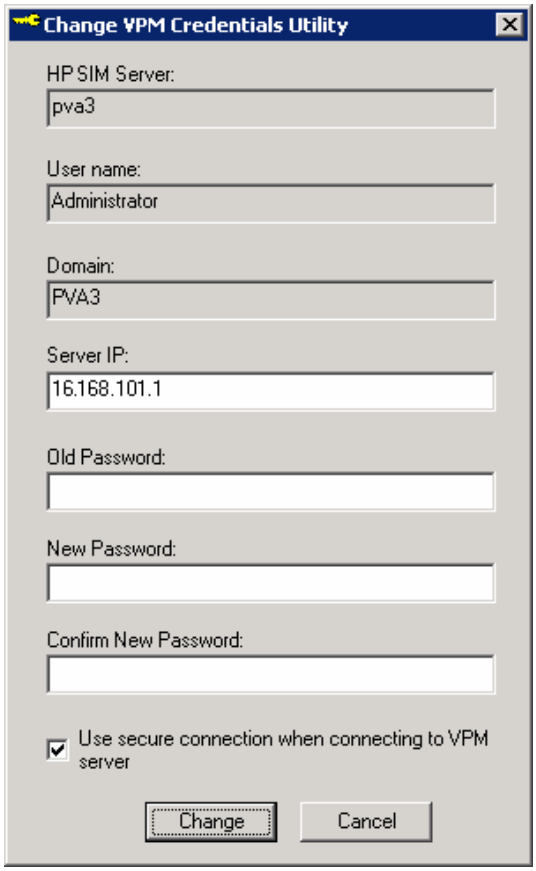
- When the credentials or IP address of the HP SIM server have been changed
- When the credentials of the account used to install Vulnerability and Patch Management Pack have been changed
- To turn on or off the secure connection between the HP SIM and VPM server

To update the Vulnerability and Patch Management Pack credentials:

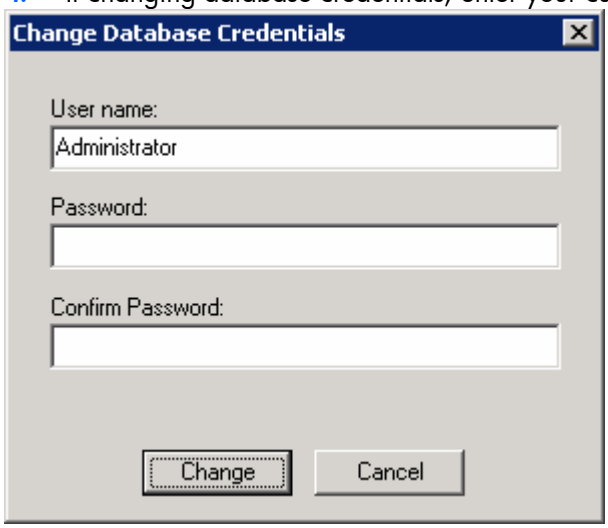
1. From the VPM server, click **Start>HP Vulnerability and Patch Management Pack>Change VPM Credentials.**
2. Select whether to change Vulnerability and Patch Management Pack or database credentials, and click **OK.**



3. If changing Vulnerability and Patch Management Pack credentials, enter your current user credentials and IP address, select whether to a secure connection to the VPM server, and click **Change.**



4. If changing database credentials, enter your current database credentials, and click **Change.**



Backing up and restoring Vulnerability and Patch Management Pack

Introduction

Vulnerability and Patch Management Pack application files are tightly coupled to HP SIM and its components. There are also Vulnerability and Patch Management Pack subcomponents, which can place files in other locations. A number of tables exist in databases, which require special tools to back up effectively.

Use the following guidelines to preserve the history of previous scan results and the list of patches installed on each target system.

The Vulnerability and Patch Management Pack plug-in for HP SIM can be installed in a shared or distributed configuration. Backup and restore can be done by preserving individual components. Before beginning:

- Understand the HP SIM file/directory structure and database layout
- Understand the Vulnerability and Patch Management Pack file/directory structure

Component backup

HP SIM must be offline to back up components. To back up individual components:

1. Back up the Vulnerability and Patch Management Pack files under the HP SIM directory:
   - C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\home\STATConfigurations
   - C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\home\STATScanner
2. Back up HP SIM directory tree and the HP SIM database. For instructions, see the *HP Systems Insight Manager Help Guide*. This procedure might be different depending on the operating system.

Component restoration

1. Restore HP SIM and the HP SIM database from the backup files.
2. Install Vulnerability and Patch Management Pack.
3. Restore the Vulnerability and Patch Management Pack files from the backup.

This procedure restores the Vulnerability and Patch Management Pack historical scan and patch data to the point where it was backed up. HP recommends running a scan to restore current Vulnerability and Patch Management Pack status.

Vulnerability and Patch Management Pack events

Vulnerability and Patch Management Pack creates events in HP SIM. These events can be viewed with all HP SIM events in the Events list, or independently in the VPM Events list.

Scan events

Table 6 lists the events created by the Vulnerability and Patch Management Pack scanning components.

Table 6 VPM scan events

Event	Description	Occurs
Submitted VPM Scan	A vulnerability scan has been submitted	When a scan is submitted. If another scan is already running, this scan is queued.
Started VPM Scan	A group vulnerability scan has started	When a scan is started for all systems selected in the scan operation. Each individual system also has a scan start event. Individual machines are scanned one at a time.
Started VPM Scan for System	A vulnerability scan has started on a system	At the start of the scan for each individual system.
Completed VPM Scan	A group vulnerability scan has completed	When a scan is completed for all systems selected in the scan operation. Each individual system also has a scan completion event. Individual machines are scanned one at a time.
Completed VPM Scan for System	A vulnerability scan has completed on a system	At the completion of the scan for each individual system.
Failed VPM Scan	A failure has occurred during a VPM scan	When an entire scan fails to complete because of an internal error. Check the system event log for more information.
Failed VPM Scan for a System	A failure has occurred during a VPM scan for a particular system	When an individual system scan fails to complete because of an internal error. Check the system event log for more information

Patch and fix events

Table 7 lists the events created by the Vulnerability and Patch Management Pack patching components.

Table 7 VPM patch and fix events

Event	Description	Occurs
Submitted VPM Patch and Fix	A VPM patch and fix has been submitted.	When one more patches and fixes have been submitted.
Started VPM Patch and Fix	A group VPM patch and fix has started.	When one or more patches or fixes have been started for all systems selected in the patch-fix operation. Each individual system also has a start event.
Started VPM Patch and Fix for System	A VPM patch and fix has started on a system.	When one or more patches or fixes have been started for an individual system.
Completed VPM Patch and Fix	A group VPM patch and fix has completed.	When all patches and fixes have been completed for all systems selected in the patch-fix operation. Each individual system also has a completion event.
VPM Patch Start	A vulnerability patch installation has begun on the target system	When a vulnerability patch installation has been started on the target system. A software update or bulletin is being applied to the target system.
Completed VPM Patch and Fix for System	A VPM patch and fix has completed on a system.	When all patches and fixes have been completed for an individual system.
VPM Patch Ended with Success	A vulnerability patch installation has ended on the target system with the status of successful.	When a vulnerability patch installation has ended on the target system with the status of successful.
VPM Patch Ended with Failure	A vulnerability patch installation has ended on the target system with the status of failure.	When a vulnerability patch installation has ended on the target system with the status of failure. Follow up might be required to determine the actual cause and remedy to the failure. It might be useful to examine any patch event details related to this patch.
VPM Patch Current Status	VPM Patch Agent is reporting the current status of a patch on the target device.	The status is reported after the reboot. When VPM Patch Agent reports the current status of a patch on the target device because of a patch requiring a reboot.
VPM Patch Not Applicable	The selected patch is not applicable to the selected system and therefore is not applied.	When the selected patch is not applicable to the selected system.
Failed VPM Patch and Fix	A failure has occurred during a VPM patch or fix operation.	This event occurs when one or more patches fails to complete because of an internal error. Check the system event log for more information.

Table 7 VPM patch and fix events

Event	Description	Occurs
Failed VPM Patch and Fix for a System	A failure has occurred during a VPM patch or fix operation for a particular system.	When an individual system fix fails to complete because of an internal error. Check the system event log for more information.

Acquisition events

Table 8 lists the events created by the Vulnerability and Patch Management Pack patch acquisition.

Table 8 VPM acquisition events

Event	Description	Occurs
Started VPM Acquisition	Acquisition of vulnerability updates and patches has started	When acquisition of scan definitions, patches and fixes for selected operating systems and applications has started. This operation might take a while depending on the number of items being downloaded.
VPM has been Updated	The VPM product has been updated	When patches for selected operating systems and applications have been downloaded successfully as part of an acquisition.
VPM Scan Definitions Updated	Successfully updated vulnerability scan definitions	When scan definition files have been updated successfully as part of an acquisition.
VPM / STAT Updated	Successfully updated the vulnerability scanner component of VPM	When code that scans and fixes configuration issues has been updated successfully as part of an acquisition.
VPM Scan Definitions Up-to-date	No updates required for the vulnerability scan definitions, already up to date	When scan definition files did not need to be updated as part of an acquisition.
VPM / STAT Up-to-date	No updates required for the vulnerability scanner component of VPM, already up to date	When code that scans and fixes configuration issues did not need to be updated as part of an acquisition.
Completed VPM Acquisition	Acquisition of vulnerability updates and patches has completed	When acquisition of scan definitions, patches, and fixes for selected operating systems and applications is complete.
Failed VPM Acquisition	A failure has occurred during a VPM patch acquisition	When acquisition of scan definitions, patches, and fixes for selected operating systems and applications failed.
Failed VPM Scan Definitions Update	Updates for the vulnerability scan definitions failed	When acquisition of scan definitions has failed.
Failed VPM / STAT Update	Updates for the vulnerability scanner component of VPM failed	When acquisition of updated code that scans and fixes configuration issues failed.

Miscellaneous events

Table 9 lists the miscellaneous events created by Vulnerability and Patch Management Pack.

Table 9 Miscellaneous VPM events

Event	Description	Occurs
Installed VPM	VPM has been installed	When installation of VPM successfully completes.
Removed VPM	The VPM product has been removed from this HP SIM Server	When uninstallation of VPM successfully completes.
VPM Product License	VPM license applied	When a license for VPM is successfully applied to HP SIM.
VPM Product License Failure	VPM license not applied	When a license for VPM is not successfully applied to HP SIM.
VPM Security Access Violation	VPM is reporting a security violation	When the VPM plug-in (on the HP SIM server) does not have the right credentials to access the STAT Scanner service (on the VPM server).
VPM Scan Definition Creation Failure	VPM could not write a new vulnerability scan definition file	When a custom scan definition cannot be created. This event can indicate a lack of disk space or permission problems.
VPM Scan Definition Removal Failure	VPM could not remove a vulnerability scan definition file	When one or more custom scan definitions are not removed as a part of the delete operation from the Customize Scan operation.
VPM Scanner Service Unreachable	VPM could not make a connection to the vulnerability scanner service	When VPM has found a problem trying to contact the STAT Scanner service either because of a network problem or because STAT Scanner service is not operational (for example, IIS service is not running on the VPM server).
VPM Results Structure Creation Failure	VPM could not create its results directory	When VPM cannot create the directory structure required to receive the scan results.
VPM Results Creation Failure	VPM could not write a results file	When a custom scan definition cannot be created. This event can indicate a lack of disk space or permission problems.
VPM Results Removal Failure	VPM failed to remove a results file from the VPM results area	When one or more reports are not removed as a part of the delete operation from the View Results by System or View Results by Scan Name process.
Installed VPM Patch Agent	The VPM Patch Agent has been installed	When the VPM Patch Agent deploys successfully to a system as part of a licensing operation or the Deploy VPM Patch Agent operation.

Table 9 Miscellaneous VPM events

Event	Description	Occurs
Failed VPM Patch Agent Install	A failure has occurred in the VPM Patch Agent installation	When the VPM Patch Agent fails to deploy to a system as part of a licensing operation or the Deploy VPM Patch Agent operation. VPM might not have permission to access the system. If the system type is Unknown or Unmanaged, the VPM Patch Agent must be deployed from the Deploy VPM Patch Agent menu so the operating system type can be manually selected.
Started VPM Patch Removal	A patch removal operation has been started	When removal of a patch starts.
Completed VPM Patch Removal	A patch removal operation has completed	When a patch is successfully removed from a system.
VPM Generic Radia Error	An error has been detected in the Radia Patch Manager component of VPM	When an error occurs while attempting to apply a patch. See the event details for more information.
VPM Generic Internal Error	An internal error has been detected in VPM	When some unexpected error occurs during normal VPM operation. Some internal events have minor severity and might not cause problems to normal operation. However, critical events should be analyzed thoroughly.

HP services and technical support

Vulnerability and Patch Management Pack is offered exclusively as a part of Insight Control Environment and Insight Control Environment for BladeSystem. Starting in July 2007, Insight Control Environment suites will include one year of 24 x 7 HP Software Technical Support and Update Service.

This service provides access to HP technical resources to help you resolve software implementation or operational issues. This service also provides access to software updates and reference manuals either in electronic format or on physical media as they are made available from HP.

With this service, Insight Control Environment and Insight Control Environment for BladeSystem customers will benefit from expedited problem resolution and proactive notification and delivery of Insight Control Management software updates.

To activate your HP Software Technical Support and Update Service for Insight Control and Insight Control Environment for BladeSystem, you must register your software purchase through the HP website at **http://www.hp.com/go/ice**.

Failure to register your service will jeopardize service fulfillment.

Your Service Agreement Identifier (SAID) will be delivered to you after registration. After you have received your SAID, you can go to the software update manager (SUM) web page to view your contract online and elect electronic delivery (in addition to standard media-based updates). For more information about this service, see **http://www.hp.com/services/insight**.

In addition to the new Software Technical Support and Update Service, HP also offers a number of additional software support services, many of which are provided to our customers at no additional charge.

- **Warranty**—HP will replace defective delivery media for a period of 90 days from the **date of purchase**. This warranty applies to all Insight Control Management, HP Systems Insight Manager, and ProLiant Essentials products.
- **Startup technical software support**—Phone support is available to help you with basic installation, set-up, and usage questions. This support is provided by the knowledgeable HP Insight Control Management and Systems Insight Manager specialists' team and is available for no additional charge up to 90 days from the **date of purchase** of your server. For support in the U.S., call 1-800-HP-INVENT (1-800-474-6836). (When prompted, say "Insight Manager, P2P, and SMP.") HP Worldwide support numbers for HP SIM, P2P, and SMP are available at **http://www.hp.com/country /us/en/wwcontact.html**.
- **Join the discussion** (**http://forums.itrc.hp.com**)—The HP Support Forum is a community-based, user-supported tool for HP customers to participate in discussions among customers about HP products. For discussions related to Insight Control and ProLiant Essentials software, click **Management software and system tools**.
- **Software and Drivers download pages** (**http://www.hp.com/support**)—These pages provide the latest software and drivers for your ProLiant products.
- **Management Security** (**http://www.hp.com/servers/manage/security**)—HP is proactive in its approach to the quality and security of all its management software. Be sure to check this website often for the latest downloadable security updates.

- **Obtain the latest SmartStart** (http://www.hp.com/servers/smartstart)—The SmartStart, Management, and Firmware CDs are now available for download by registering at the SmartStart website. If you wish to receive physical kits with each release, you can order single release kits from the SmartStart website. To receive proactive notification when SmartStart releases are available, subscribe to Subscriber's Choice at http://www.hp.com/go/subscriberschoice.

Index

L

M

O

P

R

S

T

U

V

W